# Federal Bureau of Investigation


## Privacy Impact Assessment
for the
National Instant Criminal Background Check System (NICS)

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, U.S. Department of Justice

Date approved: [November 6, 2019]

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

# EXECUTIVE SUMMARY

The National Instant Criminal Background Check System (NICS) is a national system established pursuant to the Brady Handgun Violence Prevention Act of 1993 (Brady Act) which provides a means of checking available information to make an immediate determination as to whether a person is disqualified from possessing or receiving a firearm or permit by federal or state law. In 2016, the NICS was enhanced with a new, Internet-accessible system, capable of operating on a continuous 24 hours a day, 7 days a week, 365 days a year basis. Much of the functionality of the previous system has been automated. A major efficiency gained was the consolidation of disparate databases, applications, and systems into one central location. Users access the system based on the privileges established by virtue of their user role. This Privacy Impact Assessment discusses the privacy risks associated with the NICS and permissible uses of information collected by, and maintained within, the NICS.

# Section 1: Description of the Information System[1]

### *(a) The Purpose that the Records and/or System are Designed to Serve*

The Brady Act (Public Law. 103-159, 18 United States Code, Section 922) requires a Federal Firearms Licensee (FFL) to contact the NICS to initiate a background check before transferring a firearm to an unlicensed person. The Gun Control Act of 1968 and the Bureau of Alcohol, Tobacco, Firearms and Explosive's (ATF) regulatory implementation of the Gun Control Act requires a buyer to complete an ATF Form 4473 in the presence of authorized FFL personnel in order to purchase one or more firearms. Title 28, Code of Federal Regulations (C.F.R.), Section 25.6 requires the FFL to provide specified information to the NICS. Additionally, per 28 C.F.R. § 25.6(j), criminal justice agencies may access the NICS in conjunction with the return of firearms to rightful owners and the issuance of firearms and explosives-related permits. The ATF has access to the NICS in conjunction with the issuance of explosives permits and licenses; and, the NICS may respond to ATF queries in connection with its investigative activities pursuant to the Gun Control Act and the National Firearms Act of 1938. Finally, per special act of Congress, 42 U.S.C. § 2201a(c), the Nuclear Regulatory Commission may utilize the NICS to run background checks on certain categories of its personnel. Further expansion of authorized NICS uses may occur in the future.

### *(b) The Way the System Operates to Achieve the Purpose*

The NICS is a national system that queries available records in the National Crime Information Center (NCIC), the Interstate Identification Index (III), the NICS Indices, and, for a non-US citizen, the information systems maintained by the U.S. Immigration and Customs Enforcement (ICE) in the U.S. Department of Homeland Security. The intent of such NICS queries is to determine whether prospective firearm purchasers or firearm permit applicants[2] are disqualified from receiving firearms or

[1] Additional Law Enforcement Sensitive information about the NICS is contained in an unpublished appendix to this Privacy Impact Assessment.
[2] The NICS Section does not process firearm permit applications; however, authorized states do.

associated permits. The NICS is intended to provide the FFLs with an immediate determination as to whether the transfer of a firearm may proceed, is denied, or if more research is required to determine if the transfer would violate federal or state law.

In order to process name-based background checks, when a transaction is initiated, the NICS simultaneously queries all available records in the NCIC, the III, the NICS Indices, and, in instances where the prospective transferee is a non-U.S. citizen, the information systems maintained by the ICE. If a NICS query results in a valid match to an individual included in the NCIC, the III, the NICS Indices, or the ICE databases, but the available information is not sufficient to determine if the transfer of a firearm is prohibited, a secondary search of other databases, such as the Disposition Document File (DDF), the Voluntary Appeal File (VAF) Database, the ATF Relief of Disabilities Database, and other available FBI, federal, regional, and state databases and websites is conducted. In the process of making the final determination, NICS users consider records collected by the FBI from federal, state, local, tribal, foreign, and international agencies/organizations, or other entities, to determine if individuals are prohibited by federal law[3] from possessing or receiving a firearm, explosive, or permit. These records may include an individual's name; sex; race; other personal descriptive data; complete date of birth (DOB); state of residence; sometimes a unique identifying number, such as a Social Security Number (SSN) (but the 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, other interaction with the criminal justice system, or involuntary commitment.

Information found through primary and secondary searches can be used to determine whether prospective firearm transferees, firearm permit applicants, or explosives transferees can lawfully receive firearms, explosives, or associated permits. In cases where a NICS search does not produce a record signifying that a transferee is, or may be, prohibited from possessing or receiving a firearm, explosive, or permit under federal or state law, the FFL is advised that the transaction may "proceed." If the search hits on a record that potentially matches the transferee, the NICS Section or the NICS Point of Contact (POC)[4] will review the record to determine if it matches the prospective transferee, if the matching record is complete, and whether a matching record indicates that the transferee is a prohibited person. If the record indicates ineligibility, the FFL is instructed to "deny" the transaction; and if the record is incomplete or inconclusive, the FFL is advised that the transaction has been "delayed" for further review. In the case of a "delayed" transaction, attempts are made to obtain sufficient information to give the transaction a final status.

---

[3] Federal law also includes a prohibition for individuals who are prohibited from possessing or receiving a firearm on the basis of state law. See 18 U.S.C. §§ 922t(2), 922t(4).

[4] A POC 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 receives NICS background check requests from FFLs, checks state or local record systems, performs the 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 has 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 the state's handgun transfers, while the FBI performs the checks for its long gun transfers.

Absent a denial, in accordance with the Brady Act, it is not unlawful for an FFL to transfer a firearm after the third business day, even if the FBI Criminal Justice Information Services Division's NICS Section has been unable to provide a "proceed" response. If the NICS Section is unable to determine whether a delayed transaction should be denied within three business days of a background check, the FFL is not prohibited from transferring the firearm, if state law allows, pursuant to 18 U.S.C. § 922(t)(1). Regardless of whether the transfer occurs, the NICS Section continues to seek information to reach a final determination on a "delayed" transaction. In cases where prohibiting information regarding a delayed transaction is received more than three business days after the check was initiated, the FBI contacts the FFL to change the status from "delayed" to "denied." If the FFL has already transferred the firearm, the FBI refers the transaction to the ATF to investigate and possibly retrieve the firearm.

The information contained in the databases which respond to the NICS is critical for the NICS Section and NICS POCs to make accurate determinations as to whether an individual is prohibited by federal or state law from possessing a firearm, explosive, or permit. The NICS can automatically proceed or deny the purchase of firearms without a person viewing the transaction. The thresholds for determining what constitutes an auto-proceed or auto-deny have been configured and can be adjusted. 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.

***(c) The Type of Information Collected, Maintained, Used, or Disseminated by the System and Access to the Information***

The NICS collects and maintains information regarding a variety of individuals involved in the NICS background check process including potential transferees; individuals prohibited from possessing a firearm; individuals challenging a NICS denial or delay; individuals requesting that their information be retained by the NICS; FFLs; FBI employees and employees of POC states or other law enforcement agencies; individuals granted relief from a firearms or explosives-related disability and/or granted a pardon; and individuals under investigation for criminal or civil violations that may come to light during the course of a NICS check. Records on these individuals may include biographic and biometric information such as names, phone numbers, addresses, email addresses, sex, race, DOBs, state(s) of residence, unique identifying numbers (such as an SSN, military number, or number assigned by federal, state, local, or other authorities), other personal descriptive data (such as height, weight, eye and hair color, and place of birth), and fingerprints. The information is stored in one system platform, which houses the formerly disparate databases, applications, and systems of: (1) the NICS E-Check; (2) the NICS Indices; (3) the NICS Audit Log; (4) the Appeals Management Database (AMD); (5) the VAF; (6) the FFL File; (7) the Automatic Call Distribution (ACD) System and Fax Server; and (8) the Subject of Interest (SOI) Database.[5] In addition, the NICS relies on (9) the DDF and (10) the ATF Relief of Disabilities Database. These latter databases (9 and 10) do not contain any indicators of the NICS activity (any indicators are scrubbed from the records that are kept), and are not automatically checked during transaction queries.

---

[5] Information about the SOI Database is set forth in the appendix to this Privacy Impact Assessment.

Generally, information in the NICS is available only to authorized NICS personnel, other FBI personnel (employees, contractors) supporting NICS functions, authorized POC/partial-POC states, and other entities authorized to conduct NICS checks. Specific portions of the NICS may be available to other individuals, agencies, and entities, as outlined below. NICS employs role-based access controls for users. For users within the NICS Section, each user has an established profile which provides capabilities based on the need/function of the user's assigned unit or team. Changes in a user's assigned unit or team are reflected in their profile and role-based access is adjusted accordingly. Audit logs capture which users access which information in the NICS, and all NICS users are audited.

Below is a description of the above databases, applications, and systems, and who has access to what information:

**(1) The NICS E-Check**

The NICS E-Check was established to meet the legal requirement set forth in Section 103(b) of the Brady Act requiring the NICS to provide other electronic means of conducting background checks, in addition to telephone calls. Historically, the majority of the NICS checks have been initiated by FFLs via the telephone. To initiate a NICS check by phone, an FFL contacts the NICS through the NICS Contracted Call Center and conveys information to a Customer Service Representative (CSR). The CSR validates the FFL's identity by obtaining the FFL's license number and code word. Once validation is complete, the FFL transmits information supplied by the firearm purchaser on the ATF Form 4473 (e.g., name, sex, race, DOB, state of residence). The CSR enters the information transmitted by the FFL into a computer terminal and initiates the background check.

The NICS E-Check provides an Internet access point through which FFLs, and other entities authorized to conduct the NICS checks, can electronically initiate NICS background checks. Users can access the NICS E-Check 24 hours a day, 7 days a week, from any computer or mobile device with Internet access. The majority of NICS checks initiated by FFLs are now submitted via E-Check. The Law Enforcement Enterprise Portal (LEEP)[6] authenticates FFLs and other E-Check users. To access the NICS E-Check, FFLs register at the NICS E-Check website. The registration application requests the following information regarding the FFL: first and last name, email address, FFL number, FFL code word, FFL name of licensee business, FFL address, FFL phone number, and FFL fax number. Registration only needs to be completed one time, per FFL account. Once an FFL account is created, an owner or manager at the FFL location can create and modify accounts for additional NICS E-Check users at the FFL location. The enrollment forms are scanned and stored. The registration form itself is submitted electronically and stored within the NICS.

Once an FFL accesses the NICS E-Check, the FFL electronically submits the firearm purchaser's information from the ATF Form 4473 to the NICS. After the information is processed by the NICS Section, a status is provided to the FFL regarding the submitted transaction. The NICS E-Check allows

[6] The LEEP has separate privacy documentation.

the FFL to see the firearm purchaser's name, the NICS Transaction Number (NTN),[7] date and time searched, and the status of the transaction. After the background check is completed, the FFL will receive a status on the NTN of "Researching," "Delay," or "New." A "Researching" response indicates to the FFL the search is still being conducted by the NICS. A "Delay" response indicates that the information entered by the FFL on the individual requires more research to determine if the transfer would violate federal, state, or local laws. A "New" response indicates to the FFL the search has been completed and a response has been received from the NICS. After clicking on the "New" response, the FFL will see either a "Proceed" response (indicating, based on available information, that the transfer of a firearm to the individual is not prohibited), a "Deny" response (indicating, based on available information, that the transfer of a firearm to the individual is prohibited) or a "Cancel" response (indicating the NTN has been "Canceled" and the transfer may not take place for this specific NTN). Transaction information remains in the NICS E-Check until accepted by the FFL. Once the FFL accepts the final status of a transaction from the NICS E-Check, the transaction is deleted from the NICS E-Check database. Transactions for which the status is not picked up within 30 days are also deleted from the database. The FFLs can view the NTN History for as long as the NTN is not purged, generally up to 88 days. The NTN History contains only the NTN, date and time created, and the status of the transaction (proceed/deny). The NTN History does not contain any Personally Identifiable Information (PII) from the NICS transaction. This ensures compliance with the NICS record retention laws.

Other NICS users authorized to conduct NICS background checks may also utilize the NICS E-Check. Currently, the ATF accesses the NICS E-Check to conduct ATF re-checks, ATF Explosives and Federal Firearms Licensing Service checks, and National Firearms Act checks. The Nuclear Regulatory Commission can utilize the NICS E-Check to conduct background checks as authorized by law. Law enforcement agencies may run Disposition of Firearms checks via the NICS E-Check. Currently, background checks conducted by POC states are not initiated via the NICS E-Check. In the future, the NICS E-Check will be capable of allowing a POC state to perform their functions as a POC to include FFL transactions in POC states and state permit checks.[8]

Information in the NICS E-Check is submitted by FFLs and other users authorized to conduct NICS checks. The FFLs and authorized users have access to information they have submitted and status information regarding their submitted transactions. A user only has access to the NICS E-Check information on transactions it initiated. The NICS Section has access to all information in the NICS E-Check.

**(2) The NICS Indices, including State Prohibited Persons File**

The NICS Indices was created specifically for the NICS and contains information obtained from

---

[7] An NTN is a unique number assigned to each valid background check inquiry received by the NICS. *See* 28 C.F.R. § 25.2.
[8] The POC states currently conduct the federally required background checks via an electronic socket interface between the NICS and the NCIC. Authorized state or local law enforcement agencies may also access the NICS via the NCIC to initiate background checks. The POC states are required to provide the NICS with the final determination of the POC state transaction. The POC final determinations are sent via the NCIC/NICS connection.

federal, state, local, and tribal agencies about individuals who are prohibited by federal or state law from possessing or receiving a firearm. Individuals who are prohibited by federal law from possessing or receiving a firearm include any individual who:

A. 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 (involving the use or attempted use of physical force 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 under indictment or information for a crime punishable by imprisonment for a term exceeding one year.
K. Is otherwise disqualified from possessing a firearm under state law.

Information in the NICS Indices may include an individual's name; sex; race; DOB; state of residence; at times a unique identifier such as a SSN, a military number, or other number or alphanumeric assigned by federal, state, local, or other authorities; other personal descriptive data; and other descriptors and information supporting an entry into the NICS Indices, such as information collected as a result of arrest, conviction, incarceration, or involuntary commitment.

The NICS Indices is comprised of 12 files. Ten of the files correspond directly to federal criteria establishing persons as being prohibited from possessing or purchasing a firearm. The other two files are the State Prohibited Persons File and the Denied Persons File.

The State Prohibited Persons File is a separate, discrete file in the NICS Indices designed to house and maintain information specific to persons who are prohibited from possessing or receiving firearms based solely on state law. This is information that the states possess but have not previously had a way to enter into the NICS. The state-based information responds to a search of the NICS Indices based on a valid match of a subject's descriptive information and various other factors (e.g., the state[s] of prohibition, a state law prompting the denial, the state of purchase, the state of residence, and handgun versus long gun). Agencies contributing information to the State Prohibited Persons File, as is true with any NICS Indices submission, are responsible for updating, modifying, and canceling their data, as appropriate.

Previously, agencies were also able to place identifying information about persons prohibited into a

generic Denied Persons File. Some states have statutes that prohibit the release of the underlying basis for the prohibition; consequently, the Denied Persons File does not provide the category of the specific prohibition. However, individuals in this file are ineligible to receive and/or possess a firearm based on federal law. The Denied Persons File allowed contributors to submit records to the NICS Indices without divulging the category of prohibition. This file has been reduced in size, is being phased out, and is no longer an available file for submissions from contributors. The file will be completely eliminated in the near future.

Information in the NICS Indices regarding the subject of a NICS transaction is available to the entity dispositioning the NICS check (e.g., NICS Section, POC State, ATF). Entities submitting records to the NICS Indices have access to the records they have submitted. The NICS Section has access to all information in the NICS Indices. For auditing purposes, the CJIS Audit Unit has access to records in the NICS Indices. Federal regulation governs access to the NICS Indices for background checks other than a firearm transfer. Additional use of NICS Indices information is limited to (1) providing information to federal, state, local, or tribal criminal justice agencies in connection with the issuance of a firearm-related or explosives-related permit or license, including permits or licenses to possess, acquire, or transfer a firearm, or to carry a concealed firearm, or to import, manufacture, deal in, or purchase explosives; (2) responding to an inquiry from the ATF in connection with a civil or criminal law enforcement activity relating to the Gun Control Act or the National Firearms Act; and (3) disposing of firearms in the possession of a federal, state, local, or tribal criminal justice agency. *See* 28 C.F.R. § 25.6(j).

**(3) NICS 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. Every background check processed by the NICS is captured in the Audit Log. Consequently, the Audit Log contains information on any individual who has applied for the transfer of a firearm, explosive, or a related permit or license, or has otherwise had his or her name forwarded to the NICS as part of a request for a NICS background check as authorized by 28 C.F.R. § 25 or other federal law. The Audit Log may also contain information on individuals who have challenged a NICS transaction.

With regard to a specific NICS transaction, the Audit Log includes: the name and other identifying information about the prospective transferee or other individual submitted for a NICS check; the type of transaction (inquiry or response); transaction code data elements (e.g., line number and header); time; date of inquiry; Originating Agency Identifier (ORI)[9] of the agency completing the check; FFL identification number; inquiry/response data, such as an assigned NTN; information found by the NICS search; and the reason for a denial, if an individual is denied. If a NICS transaction requires research outside of the NCIC, the III, and the NICS Indices, any relevant information on a potential transferee found during research may be attached to the transaction and stored in the Audit Log. This may include documents received from criminal justice and other agencies (e.g., arrest reports, court

[9] An ORI is a nine-character identifier assigned by the FBI to an agency that has met the established qualifying criteria for ORI assignment to identify the agency in transactions on the NCIC System.

transcripts, disposition information, information regarding involuntary commitments, court orders).

NICS transactions that result in a proceed response are purged 24 hours from the time the response is communicated to the FFL because proceeded transactions must be promptly purged[10] of all identifying information submitted by or on behalf of the transferee. For proceeded transactions, all that remains in the Audit Log is the NTN, the date and time of the transaction (i.e., creation of the NTN), status, state of purchase, Purpose ID,[11] notification date, source, and the FFL identification number. Within 90 days (usually by the 88th day) from the issuance of a proceed decision, a second purge[12] occurs and the only information that remains in the Audit Log for a proceeded transaction is the NTN and the date of the transaction. For denied transactions, all information in the Audit Log is retained. If a transaction is not proceeded or denied by the 88th day, all identifying information is purged from the Audit Log and only the NTN and the date of the transaction remain.

The use of information in the NICS Audit Log is controlled by regulation. *See* 28 C.F.R. §25.9(b)(2). Generally, access to information in the NICS Audit Log is available to NICS personnel to analyze system performance, assist users in resolving operational problems, support the firearms-related challenge process, or support audits of the use and performance of the system. Information on denied transactions is pushed to the NCIC's NICS Denied Transaction File where it is available to federal, state, local, tribal, and territorial criminal justice agencies. While researching a transaction, information regarding an individual undergoing a NICS check (e.g., name, DOB, SSN, criminal history information) may be shared with federal, state, local, tribal, territorial and other entities and organizations to elicit information to help determine whether to proceed or deny the NICS transaction. Contractors researching delayed transactions on behalf of the NICS Section may retrieve limited information from the NICS Audit Log via the NICS E-Check portal on the LEEP.

The use of NICS Audit Log information about proceeded transactions is restricted to FBI employees for the purpose of conducting audits of the use and performance of the NICS and for the purposes outlined in 28 C.F.R. § 25.9(b)(2)(i) and (ii): "(i) information in the NICS Audit Log, including information not yet destroyed under § 25.9(b)(1)(iii), that indicates, either on its face or in conjunction with other information, a violation or potential violation of law or regulation, may be shared with appropriate authorities responsible for investigating, prosecuting, and/or enforcing such law or regulation; and (ii) the NTNs and dates for allowed transactions may be shared with the ATF in individual FFL Audit Logs as specified in § 25.9(b)(4)."

---

[10] Per 28 C.F.R. § 25.9(b)(1)(iii), in cases of the NICS Audit Log records relating to allowed transactions, all identifying information submitted by or on behalf of the transferee will be destroyed within 24 hours after the FFL receives communication of the determination that the transfer may proceed. 18 U.S.C. § 922(t)(2)(C) and Pub. L. 112-55, § 511, 125 Stat. 552 (2011).

[11] A Purpose ID is a unique identifier which identifies the reason or purpose of the background check (e.g., 01-sale of handgun, 02-sale of long gun, 05-prepawn of hand gun).

[12] PL 112-55 requires the destruction of "all identifying information provided by or on behalf of any person who has been determined not to be prohibited" within 24 hours, which leaves the FFL number and the date and time of the transaction in the system until the time of the original FBI purge plan. In order to comply with the Brady Act's requirement to destroy all proceed transaction records except the NTN and the date that the NTN was created, a second purge takes place at 88 days.

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 report 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 identification number, and creation date and time for cancelled, open, and delayed transactions. With respect to proceed transactions, only the NTN and its creation date are retained in the NICS Audit Log. An individual FFL audit log may only contain up to 60 days' worth of proceeded transaction transfer records originating at the FFL. Proceeded information in the NICS Audit Log may only include information not subject to destruction pursuant to a congressionally-mandated restriction.

Authorized ATF personnel also have the ability, via the NICS E-Check on the LEEP, to directly submit a query and automatically receive information the NICS is permitted to share for individual FFL Audit Logs (e.g., all information on denied transactions conducted at a specific FFL; non-identifying information of all delayed and proceeded transactions conducted at a specific FFL). This query feature enables the ATF to obtain the individual FFL Audit Logs for inspections, but instead of a NICS Section employee manually generating the reports, the new capability allows the ATF to obtain them in an automated fashion.

**(4) Appeals Management Database (AMD)**

The NICS collects, generates, and retains firearm-related challenges, formerly known as appeal records, in the firearm-related challenge records in the AMD.[13] Information in the AMD reflects inquiries by potential transferees regarding the reason for a delay or denial by the NICS or 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. The AMD captures the individual's name, address, and gender; NTN or State Transaction Number (if one was assigned); state of purchase; state of residence; name of the NICS Examiner or other FBI employee/contractor working the case; status of the stage of processing for the firearm-related challenge case; the projected date the firearm-related challenge will purge from the system; type of incoming and outgoing correspondence; the result of the firearm-related challenge (e.g., whether the denial was affirmed or overturned); and the date the firearm-related challenge was closed. In addition, the AMD retains any information submitted by the potential transferee in support of his or her inquiry or firearm-related challenge which may include fingerprints, court documents, pardons, restorations, and identification documents. In addition to information about appellants, the AMD may contain information on other individuals pertinent to an inquiry or firearm-related challenge, such as contact information for an appellant's counsel or record-owning agency.

Information in the AMD is directly available to FBI personnel involved in processing and resolving firearm-related challenges. Information from the AMD may be provided to the individual about whom the information pertains and such individual's representative. Information may also be provided to members of Congress with written consent of the individual about whom the information pertains.

---

[13] The AMD is separate from the Voluntary Appeal File because they have different functions and retention rules.

**(5) Voluntary Appeal File (VAF)**

Pursuant to 28 C.F.R. § 25.10(g), the VAF was established as a separate NICS-internal database to prevent future unnecessary delays or erroneous denials in firearms transactions. As stated above, the NICS must destroy[14] 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 or state law. If a potential purchaser is delayed or denied a firearm and successfully challenges the decision, the NICS cannot retain the record of the challenge or the supporting documentation for more than 90 days unless the information is maintained as part of the VAF.

Because of mandatory purge requirements, individuals who wish to make subsequent purchases may be delayed or denied again for many reasons (such as similarity of their personal information to that of other persons in NICS-consulted databases) until their record has been re-reviewed or until the individual has initiated a challenge. The NICS regulations, 28 C.F.R. § 25, permit lawful transferees to request that the NICS maintain certain personal information in the VAF. The VAF may maintain information on individuals who have provided the FBI with written consent to maintain information about themselves in the VAF. 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 the VAF. However, if a VAF applicant is determined not to be firearms-prohibited, his/her PII is maintained, and he/she is issued a VAF Unique Personal Identification Number (UPIN). When a potential transferee presents his/her UPIN to an FFL, the NICS will include a review of the VAF in the related background check.

The PII in the VAF is used for the limited purpose of clarifying existing records and/or proving identity to facilitate future transactions. Data in the VAF may include, but is not limited to, name, DOB, SSN, address, email address, phone number, place of birth, state of residence, general descriptive data (e.g., height, weight, eye color, hair color), fingerprint cards, photographs, court documentation, correspondence, and information contained in the applicant's challenge file, if one exists. Fingerprints are required to ensure the individual does not have a prohibiting criminal offense. Whether rolled fingerprint cards or electronic scans of fingerprint impressions are submitted, they must be prepared by law enforcement or another authorized fingerprinting agency with a stamp or other official indication of the agency's name, address, and telephone number in the designated area of the fingerprint card. All VAF records are kept only in electronic format. Fingerprint cards mailed to the FBI are electronically scanned and attached to the individual's record in the VAF. The hard copy of the fingerprint cards are then destroyed, or, if requested by the applicant, returned to the individual.

As discussed below, individuals applying for inclusion in the VAF have the ability to electronically

---

[14] Per 28 C.F.R. § 25.9(b)(1)(iii), in cases of the NICS Audit Log records relating to allowed transactions, all identifying information submitted by or on behalf of the transferee will be destroyed within 24 hours after the FFL receives communication of the determination that the transfer may proceed. 18 U.S.C. § 922(t)(2)(C) and Pub. L. 112-55, § 511, 125 Stat. 552 (2011).

submit information to the VAF. Individuals have access only to submit their own information in the VAF and view the information they have submitted and messages regarding the status of their VAF application. FBI personnel involved in processing firearm-related challenges can query the VAF. NICS Section employees who process applications for entry into the VAF have direct access to all information in the VAF, including pending applications.

NICS Section employees processing transactions have direct access to VAF information about individuals approved for inclusion in the VAF. NICS Section employees search the VAF for supplemental information that could assist in resolving a delayed firearm or explosive transaction immediately, without the need for contacting outside entities or performing other research. Review of the VAF is undertaken only after a potential transferee's information results in a hit against a record in the III, the NCIC, the NICS Indices, or the ICE databases and, as noted above, when the individual has presented a UPIN to the FFL. Information on individuals approved for inclusion in the VAF is available to POC and partial-POC states via the State Information Sharing Initiative (SISI). This enhanced information resource helps foster nationwide consistency in firearms and explosives eligibility determinations.

**(6) FFL File**

The NICS also retains information about individuals who have registered with the ATF to be FFLs. This information is provided to the NICS by the ATF from the FFL application and includes the FFL's name, code word,[15] address, phone number(s), the 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 NICS has the capability to permit the ATF to provide real-time updates to FFL registration and license statuses via secure, encrypted Internet access.

Access to the FFL file is limited to the ATF and authorized FBI personnel. The NICS receives and transfers information for the FFL file through a NICS/ATF interface. The ATF's electronic transmission of information to the NICS synchronizes FFL information between the NICS and the ATF. The ATF is responsible for maintaining the list of valid FFL numbers issued to FFLs that may legally transfer firearms in the United States (i.e., gun dealers, pawnbrokers, importers, and manufacturers) as well as all necessary contact information for the FFL. The ATF also provides updates to the NICS on FFL contact information, new licenses issued, renewals, and expirations. Finally, the ATF also notifies the NICS when an FFL should be removed. The NICS uses FFL data to validate FFLs requesting Brady Law background checks on potential firearm purchasers. The ATF also notifies the FBI of time-sensitive updates to FFL information (e.g., the revocation or reinstatement of a license) via telephone or facsimile.

[15] A code word is used by the FFL when interacting with the NICS Call Center or with a NICS Section employee on the phone. The code word is also used by an FFL when conducting a check on the NICS E-Check; the FFL has to have both the code word and a password in order to gain access to the NICS E-Check.

**(7) ACD System and Fax Server**

Two computer systems are used for telephonic and fax transmissions made into and out of the NICS during system operations—the ACD System and the Fax Server. The ACD System[16] operates as a call-routing mechanism that analyzes information on calls referred from the NICS Call Center to the NICS Section and directs customer service calls to the most appropriate CSR. The ACD System records and retains the incoming phone call and associated data in the phone system, such as the incoming phone number, the NICS Section employee who answered the call, and the date and time of the incoming call. When the ACD System answers a call, the caller chooses options through Interactive Voice Response (IVR).[17] Based on the options chosen by the caller in the IVR, along with the caller's phone number (Automatic Number Identification) and the number the caller dialed (Dialed Number Identification Service), the ACD system routes calls to the appropriate personnel.

The Fax Server operates in a similar fashion. When a NICS Section employee faxes a request for information, his/her outgoing fax transmission contains a control number that identifies the NICS transaction. The reply fax transmission also contains that control number. The Fax Server automatically directs the return fax transmission to the appropriate transaction. 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. Information received via the Fax Server may include any information pertinent to determining whether an individual is prohibited by federal or state law from receiving a firearm, explosive, or related permit, such as arrest reports, court transcripts, disposition information, information regarding involuntary commitments, or court orders. Automation and integration for the fax routing system reduces the manual investigation needed to find the recipient of unrouteable faxes and the routing of these faxes. The system scans the incoming fax for the assigned serial number and, if found, attaches the fax to the corresponding transaction. If information is not found, the fax can manually be routed to the transaction.

Information transmitted to the NICS via the ACD System and Fax Server ultimately attaches to a NICS transaction. Once attached to a NICS transaction, the information is accessed as part of the NICS Audit Log. Information received via the Fax Server as part of research is also processed (e.g., all NICS indicators are removed) and sent to the DDF. Once part of the DDF, information is available to FBI personnel, POC states, and other entities authorized to conduct NICS checks.

**(9) Disposition Document File (DDF)**

The DDF contains information that cannot be posted to a subject's criminal history record in the III or otherwise updated in the Next Generation Identification (NGI) System, or cannot be posted to other pertinent databases. The DDF is not part of the NICS; rather, it is under the control of the CJIS

---

[16] The ACD System is part of the Enterprise Telecommunications Infrastructure System (ETIS). The ETIS has separate privacy documentation available at https://www.fbi.gov/file-repository/pia-enterprise-telecommunications-infrastructure-system.pdf/view.

[17] IVR allows callers to select options that will help the ACD route their calls to the correct person (e.g., an FFL pressing one to initiate a new transaction, or pressing two to check the status of a pending transaction).

Division's Biometric Services Section (BSS). Records found in the DDF may include, but are not limited to, arrest dispositions, warrants, protection orders, police reports, transcripts, court-ordered mental commitments, protection orders, and indictments and informations (if not already posted to an individual's "identity history summary," formerly known as "rap sheet"). The DDF helps reduce the need for the NICS Section and other CJIS Division personnel to contact federal, state, local, tribal, or other agencies multiple times to obtain information already provided to the FBI. Some of the information contained in the DDF is data that may be rejected from inclusion in other databases for various reasons, such as: the dates of arrest are not provided; a disposition or other information cannot be matched to a date of arrest of record; fingerprints are illegible; or validation of data, such as a stamp, seal or official signature, is lacking.

NICS Section personnel only research the DDF when a potential prohibition has been identified upon a NICS transaction hitting against a record in the III, the NCIC, the NICS Indices, or the ICE database. The DDF may contain information which could immediately result in a "proceed" or "deny" determination. The DDF data is available to the POC/partial-POC states and other entities authorized to conduct NICS checks who participate in the SISI. This enhanced information resource helps foster nationwide consistency in firearms and explosives eligibility determinations.

The NICS Section currently provides information received during the delayed transaction research process to the DDF via the fax server or through a third party email to the BSS. All NICS identifiers (e.g., NTN) are manually stripped from the information before it is placed in the DDF.

NICS Section personnel, POC states, the ATF, and other entities authorized to conduct NICS checks can access the DDF via the NICS. In order to receive DDF information with a NICS check, POC states and other entities authorized to conduct NICS checks must opt into the SISI. The ATF can conduct queries of and receive information from the DDF via the NICS E-Check portal on the LEEP. Other individuals, agencies, and entities may have access to information in the DDF from outside the NICS.

**(10) ATF Relief of Disabilities Database[18]**

The ATF Relief of Disabilities Database is a compilation of applicant information obtained by the ATF when it processed firearm disability relief applications from 1969 to 1992. Although the ATF stopped processing relief of disability applications in 1992, these records are retained by the NICS and are used to evaluate eligibility for firearm transactions. The ATF also processes explosive reliefs of disabilities from 2003 to present. These records are used to evaluate eligibility for explosive permit applications.

The fields contained in the ATF Relief of Disabilities Database include: the subject's name, SSN (if provided), DOB, 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.

---

[18] The ATF Relief of Disabilities Database is not subject to the Brady Act requirement to purge proceed information within 24 hours, as the ATF Relief of Disabilities Database is not part of the NICS. The Brady Act was not signed into law until 1993; the NICS first became operational on November 30, 1998.

Research of the ATF Relief of Disabilities Database is undertaken by NICS personnel only after the subject search results in a hit against a record in the III, the NCIC, the NICS Indices, or the ICE database. The ATF Relief of Disabilities Database may contain information which could immediately result in a "proceed" or "deny" determination. The POC and partial-POC states also have access to the ATF Relief of Disabilities Database. In addition, the ATF Relief of Disabilities Database is available to the ATF for research when conducting explosives checks. This enhanced information resource helps foster nationwide consistency in firearms and explosives eligibility determinations. Automation of batch submissions of ATF Relief of Disabilities Database records allows for more timely and complete updates to the information.

As with the DDF, the NICS Section personnel, POC states, the ATF, and other entities authorized to conduct NICS checks can access the ATF Relief of Disabilities Database via the NICS. The ATF can conduct queries of and receive information from the ATF Relief of Disabilities Database via the NICS E-Check portal on the LEEP. Other individuals, agencies, and entities may have access to information in the ATF Relief of Disabilities Database from outside the NICS.

***(d) How Information in the System is Retrieved by the User***

Users generally retrieve information from the NICS by a combination of personal identifiers (e.g., name, DOB, SSN) or a unique identifier for the data they seek (e.g., NTN, FFL number, AMD number). The FFLs, the ATF, and other entities authorized to conduct a NICS check can log into the NICS E-Check using a username and password or token on the LEEP page and agreeing to the NICS E-Check Terms and Conditions page. Once users select the 'Agree' button on the NICS E-Check Terms and Conditions page, they must enter their Access Number (RDS Key). The RDS Key gives the user access to the portal page where the user will initiate all their NICS work based on their user role, such as submitting a search request, checking an NTN status, and querying NTN history. During a NICS check, users provide the potential transferee's PII (e.g., name, DOB, SSN). The NICS uses the PII to check databases and returns any matching information to the NICS staff or POC state.

During a NICS check, the NICS retrieves records from the NICS Indices based on matches between the biographical data in NICS Indices records and biographical information submitted on potential transferees. Contributing agencies also have access to the records they have submitted to the NICS Indices. Those agencies that enter into the NICS Indices, via the NCIC, can retrieve their records via the Query Denied Person functionality within the NCIC. The agency can use the NICS Record Identifier[19] or Agency Record Identifier[20] to retrieve their entry. If agencies enter records via the LEEP, the agency can retrieve its NICS Indices entries by their ORI, NICS Record Identifier, Agency Record Identifier, or the name of the subject of the record. Upon request from an authorized authority, the NICS Section can provide a list of all of the agency's NICS Indices entries.

---

[19] A NICS Record Identifier is the system-generated unique number associated with each record in the NICS Indices.
[20] An Agency Record Identifier is a unique identifier assigned by the agency submitting records for inclusion in the NICS Indices.

The NICS users retrieve information from the NICS Audit Log via personnel identifier, NTN, time frame (e.g., day or month), FFL, or by a particular state or agency conducting a NICS check. Contractors researching disposition information for NICS transactions retrieve information from the delay queue based on the ORI of the agency asked to supply the disposition information.

Information from the AMD is retrieved via NICS personnel by personal identifier or AMD number.

NICS users retrieve information from the VAF via personal identifier, UPIN, or AMD number. Individuals electronically submitting information to the VAF can retrieve their information from their VAF with a unique link and PIN.

Information is entered into the FFL file by the NICS and the ATF. An FFL inquiry can be conducted using one or more of the following search criteria: FFL identification number; RDS Key; whether the FFL is listed as active by the ATF, within the NICS, or registered to use the NICS E-Check; FFL code word; license type; or any part of the FFL contact information (e.g., phone number, address, name, email, fax).

Information from the Fax Server is automatically attached to specific transactions within the NICS. Audit log information in the ACD System and Fax Server can be retrieved by keyword search.

Subjects in the SOI database can be retrieved by personal identifier or other data element in the database.

The NICS retrieves information from the DDF and ATF Relief of Disabilities Database based on matches to biographic information on potential transferees.

***(e) How Information is Transmitted to and from the System***

As discussed above, historically, the majority of the NICS checks have been initiated by FFLs via the telephone. By this method, an FFL contacts the NICS through the NICS Call Center and conveys information to a CSR. The CSR validates the FFL's identity by obtaining the FFL's license number and code word. Once validation is complete, the FFL verbally 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. With the addition of the NICS E-Check, now the method for the majority of the NICS checks, FFLs transmit information from the ATF Form 4473 to the NICS via a dedicated password-protected internet portal. The NICS E-Check also allows the ATF and other authorized entities to query the NICS and receive responsive information.

Information in the NICS Indices is electronically submitted. Agencies submitting records to the NICS Indices must have an ORI. If the agency does not have an ORI, the NICS Section will assist the agency in obtaining an ORI. Agencies have two methods to submit or maintain their NICS Indices records—either through the NCIC or the LEEP. An agency may choose to utilize the NCIC to interface with the NICS to electronically submit, modify, supplement, cancel, or display a denied individual's disqualifying information in the NICS Indices. Agencies without the NCIC capability or those who

prefer the LEEP may access the NICS Indices via the LEEP. The agency may submit NICS Indices entries by batch transfer or single entry though the LEEP connection by using the NICS E-Check icon. A LEEP account is required for the user. Once a LEEP account is established, the NICS Section can assist with the NICS E-Check activation and guide the user through the NICS Indices submission process via the NICS E-Check icon.

Firearm-related challenges are received from the individual via mail, facsimile, or email. Firearm-related challenge records are retained in the AMD. The AMD allows FBI personnel working challenges to create AMD records by having the system automatically populate information from the transaction being challenged into the new AMD record. The information contained within the AMD automatically creates outgoing correspondence.

Recently, the FBI began receiving NICS firearm-related challenge information electronically through the FBI's electronic Departmental Order process. Through a web-based portal available on <fbi.gov>, individuals can now electronically submit challenges to firearm denials and receive responses via email. The electronic challenge process has separate privacy documentation.

Individuals can submit applications for the VAF by mail or via an online portal. Once an application is received, the information is stored in the VAF and processed. Requests for additional information and correspondence regarding the status of a VAF application is available through the online portal or received by individuals via mail. If an individual uses the online portal, the NICS emails an individual when new information regarding his/her VAF application is available within the portal.

The NICS receives information found during research of delayed transactions via fax or email. Contractors researching disposition information for NICS transactions also electronically submit information to NICS via the LEEP portal. The NICS Examiners manually add notes to the NICS Audit Log.

***(f) Whether it is a Standalone System or Interconnects with Other Systems***

The NICS connects to the NCIC, the III, and the NGI System using public key infrastructure certificates. Users may also query the NCIC and the III through independent secure user interfaces. Additionally, the NICS interfaces with the LEEP for user authentication, which allows access to the NICS E-Check for authorized users, NICS Indices for submitting entities, and remote access for telework for NICS personnel. An external facing, internet accessible website allows the general public to submit VAF applications to the NICS Section and check the status of pending VAF applications. The electronic Departmental Order allows individuals to electronically file firearm-related challenges. In the future, the NICS will integrate with the NGI System to electronically send and search submitted fingerprints against the NGI System and return any matching records. The NICS may also electronically connect to the National Data Exchange (N-DEx) System and other FBI databases for secondary research using public key infrastructure certificates.

The NICS integrates with the CJIS phone system, also known as ETIS, using the PegaCall Commercial-Off-the-Shelf Integration suite, providing five main features to the users:

- Adaptive Screen Pop—Upon receipt of a call, a screen containing information relevant to the call can be displayed to a user. For example, if an FFL is calling about a specific NTN, that NTN can be displayed on the screen when the user answers the phone.

- Data Prefetch—Upon receipt of a call, information can be queried from other systems automatically. If a POC state calls in, for example, the NICS could execute queries against the NCIC and the III based on information the caller provides prior to the call being answered.

- Enhanced Call Routing—The NICS provides call routing decisions based on several criteria defined by the CJIS Division in the NICS requirement set, including the CSR skillset, transaction age, etc. For example, if a call comes in from Region 1, it is routed to NICS Examiners who are capable of working Region 1 calls. If the caller enters an NTN, the system then assigns it to the NICS Examiner working that NTN.

- Desktop Telephony— NICS personnel can control their phones directly from within the application. They can initiate or answer calls, transfer a call from the NICS Call Center to a NICS Examiner, or escalate a call to a supervisor when necessary, all from within the application.

- CSR, NICS Examiner State Management—The CSRs and NICS Examiners are able to mark themselves as "available for work" or "not available" depending on the needs of the NICS Section.

The NICS integrates with the CJIS Division Biscom services to provide incoming and outgoing fax communications. The NICS leverages Biscom Web Services to transmit outgoing faxes to their destination. For incoming faxes, the Biscom fax server conducts Optical Character Recognition based on the assigned serial number, and then routes the faxes and metadata received to the transaction and also to the DDF workbasket for additional processing.

# Section 2: Information in the System

## 2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

| **Identifying numbers** | | | | | |
|---|---|---|---|---|---|
| Social Security | X | Alien Registration | X | Financial account | |
| Taxpayer ID | | Driver's license | X | Financial transaction | |
| Employee ID | | Passport | X | Patient ID | |
| File/case ID | X | Credit card | | | |
| Other identifying numbers (specify): | | | | | |

- Military serial numbers
- Non-immigrant admission number
- Canadian Social Insurance number
- Royal Canadian Mounted Police ID or Fingerprint Section number
- Personal Identification Number (state-issued only)
- Port Security Card number
- Selective Service number
- Veterans Administration claim number
- UPIN
- AMD ID
- UCN[21]

| **General personal data** | | | | | |
|---|---|---|---|---|---|
| Name | X | Date of birth | X | Religion | |
| Maiden name | X | Place of birth | X | Financial info | |
| Alias | X | Home address | X | Medical information | |
| Gender | X | Telephone number | X | Military service | X |
| Age | X | Email address | X | Physical characteristics | X |
| Race/ethnicity | X | Education | | Mother's maiden name | X |
| Other general personal data (specify): Country and/or status of citizenship, state of residence, eye and/or hair color, height, weight. | | | | | |

| **Work-related data** | | | | | |
|---|---|---|---|---|---|
| Occupation | | Telephone number | X | Salary | |
| Job title | | Email address | X | Work history | |
| Work address | X | Business associates | X | | |
| Other work-related data (specify): Work-related data is typically provided for FFLs and NICS users. A Brady ID is assigned to each NICS Section employee. The Brady ID is utilized by the employee to identify themselves to the FFL or outside entities, rather than using their name. | | | | | |

| **Distinguishing features/Biometrics** | | | | | |
|---|---|---|---|---|---|
| Fingerprints | X | Photos | X | DNA profiles | |
| Palm prints | | Scars, marks, tattoos | X | Retina/iris scans | |
| Voice recording/signatures | | Vascular scan | | Dental profile | |

[21] A UCN, also known as an FBI Number, is a unique identification number assigned to each fingerprint submission to the Next Generation Identification system.

| **Distinguishing features/Biometrics** |
|---|
| Other distinguishing features/biometrics (specify): |

| **System admin/audit data** | | | | | |
|---|---|---|---|---|---|
| User ID | X | Date/time of access | X | ID files accessed | X |
| IP address | X | Queries run | X | Contents of files | X |
| Other system/audit data (specify): | | | | | |

| **Other information (specify)** |
|---|
| All incoming phone calls to the NICS are recorded and maintained within the ETIS. Calls are retained for 24 hours. Callers are notified their call may be recorded during the automated greeting that plays when their call is first answered. ETIS and call recordings are discussed in detail in ETIS' published Privacy Impact Assessment: <https://www.fbi.gov/file-repository/pia-enterprise-telecommunications-infrastructure-system.pdf/view> |

## 2.2 Indicate sources of the information in the system. (Check all that apply.)

| **Directly from individual about whom the information pertains** | | | | | |
|---|---|---|---|---|---|
| In person | X | Hard copy: mail/fax | X | Online | X |
| Telephone | X | Email | X | | |
| Other (specify): Although transferee information is originally provided by the individual, the NICS collects the majority of information from the FFLs; various federal, state, local, tribal, foreign, and international agencies or organizations; or other entities, including sources that may be accessed by members of the public (e.g., court records such as restraining orders, court judgments, and dispositions). | | | | | |

| **Government sources** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ components | X | Other federal entities | X |
| State, local, tribal | X | Foreign | X | | |
| Other (specify): | | | | | |

| **Non-government sources** | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, internet | | Private sector | X |
| Commercial data brokers | | | | FFLs provide the buyer | |
| Other (specify): Information from the private sector includes data the NICS receives from FFLs for firearm purchases and NICS E-Check registration. | | | | | |

## 2.3 Analysis: Now that you have identified the information collected and the

**sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)**

As discussed above, the NICS collects the majority of its information from the FFLs; various federal, state, local, tribal, foreign, or international agencies or organizations; or other entities, and not directly from the individual. Although transferees directly provide their information to FFLs, the information is conveyed to the NICS by the FFL. This creates a risk that administrative errors, such as typographical errors, may occur during data entry, which may result in a misidentification. To mitigate this risk, when FFLs provide information via telephone, the CSRs confirm the information with the FFL as they enter it into the NICS. The NICS E-Check process allows FFLs to enter the information themselves and check that information against the paper form. The firearm-related challenge process enables individuals to challenge any transfer denials and correct any misidentification through the submission of fingerprints.

Records of prohibited individuals submitted to the NICS Indices are necessarily submitted by federal, state, local, tribal, foreign, or international agencies or organizations. The entering agencies are responsible for ensuring that submitted records are timely, accurate, valid, and complete. In addition, they are responsible for the immediate correction of invalid or incorrect records. The FBI performs triennial audits of federal, state, local, and tribal agency addressing use of the NICS and entries into the NICS Indices. The audits are staggered so not all federal, state, local, and tribal agencies are audited in the same year. During the NICS Indices portion of the audit, the FBI audits a sample of entries for accuracy and validity.

The collection of information regarding individuals attempting to purchase firearms also creates a risk of the accidental creation of a firearm registry. To ensure that a firearm registry is not created, NICS stringently adheres to the 24-hour purge requirement to delete all PII on proceeded transactions. Three purge scripts are run throughout the day to purge the NICS in a timely manner. The NICS NTN purge is conducted every hour on the 20-minute mark. A non-NTN purge is completed every morning. A third purge against the database occurs nightly to purge any transaction missed during the NTN purge. The purge table status incorporates the status of each type of purge that is run for the day. The automated Daily Check report shows the purge statistics and is checked by the Operations and Maintenance Database team daily. Aggressive technical audits identify and eliminate unintentional computer logs that may provide indicators of a NICS search. Transaction logs of other systems (e.g., the NCIC, the III) redact the NICS-provided search criteria to ensure a firearm registry cannot be recreated. In addition, limited information about transactions with a proceed response is maintained in the NICS. With such transactions, all identifying information is purged within 24 hours, and within 90 days a second purge occurs leaving only the NTN and date of the transaction's creation in the system. The NICS purges automatically based on the time and date a transaction is created with the exception of transactions under appeal or with the audit flag set. Automating the purges within the system

ensures the requirements are systematically applied and reduces any errors from manual review and processing.

# Section 3: Purpose and Use of the System

## 3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

| Purpose | | | |
|---|---|---|---|
| X | For criminal law enforcement activities | X | For civil enforcement activities |
| | For intelligence activities | X | For administrative matters |
| | To conduct analysis concerning subjects of investigative or other interest | | To promote information sharing initiatives |
| | To conduct analysis to identify previously unknown areas of note, concern, or pattern | | For administering human resources programs |
| X | For litigation | | |
| X | Other (specify): The purpose of the NICS, which was established pursuant to the Brady Act, is to provide a means of checking available information to determine immediately whether a person is disqualified from possessing or receiving a firearm by federal or state law. | | |

## 3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The primary mission of the NICS is to fulfill the mandates of the Brady Act. The Brady Act requires an FFL to contact the NICS to initiate a background check before transferring a firearm to an unlicensed person. The Gun Control Act and the ATF's regulatory implementation of the Gun Control Act require a buyer to fill out an ATF Form 4473 in front of an FFL to purchase a firearm. The NICS regulations[22] require the FFL to call in specified information to the NICS.

The NICS uses the provided information to conduct a name-based search of the NCIC, the III, and the NICS Indices. The information entered on the ATF Form 4473 and provided to the NICS by the FFL allows NICS personnel to verify whether that particular individual matches any individual in the system who should be or potentially should be disqualified or prohibited from purchasing a firearm, explosive, or permit. If the subject is not a U.S. citizen, a check of the ICE databases also is conducted. If there are no hits, then a "proceed" determination will be issued to the FFL and the FFL may complete the firearm transaction. If there is a hit on a record in one or more of the databases that makes the record subject ineligible to possess or receive a firearm and the NICS verifies the match, then the NICS will issue a deny determination to the FFL and the buyer will not be permitted to buy the firearm(s).

[22] *See* 28 C.F.R. § 25.7.

Information in the VAF and the AMD allows the NICS to resolve any challenges to NICS checks and ensure future transactions are not inappropriately delayed or denied. The FFL file allows the NICS to maintain information about FFLs in order to accept information for NICS background checks. The SOI Database allows the NICS to assist law enforcement agencies which investigate, prosecute, and/or enforce violations of criminal or civil laws or regulations that may come to light during the NICS operation.

## 3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

| | Authority | Citation/Reference |
|---|---|---|
| X | Statute | 18 U.S.C. § 922, as amended by the Brady Handgun Violence Prevention Act (Brady Act) (Pub. L. 103-159, Nov. 30, 1993, codified in relevant part at 18 U.S.C. § 922(t) and 34 U.S.C. § 40901); the NICS Improvement Amendments Act of 2007 (Pub. L. 110-180, Jan. 8, 2008); Consolidated Appropriations Act ("Fix NICS Act") of 2018 (Pub. L. 115-141, March 23, 2018, codified in relevant part at 34 U.S.C. § 40901); and 28 U.S.C. § 534, as amended (Pub. L. 103-322, Title IV, 4060(a), Sep. 13, 1994, 105 Stat. 1950) |
| | Executive Order | |
| X | Federal Regulation | 28, C.F.R., § 25, Subpart A, and 28 C.F.R §0.85 |
| | Memorandum of Understanding/agreement | |
| X | Other (summarize and provide copy of relevant portion) | ATF Form 4473 |

## 3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Identifying information in proceeded transactions is purged from the system within 24 hours, and within 90 days a second purge occurs so that only the NTN and the creation date of the transaction remains. Delayed NICS transactions are purged from the system within 90 days. The NICS denial records currently are scheduled for retention for 110 years to match the CJIS Division standard. The NICS retention schedule was approved by the U.S. National Archives and Records Administration (job numbers N1-65-07-3 and N1-65-10-5).

Currently, all NICS call information is purged in 24 hours, unless the call is tagged by approved NICS personnel for auditing or investigative purposes. The NICS is currently developing Computer

Telephony Integration functionality to attach call recordings to the applicable NICS transactions. When this functionality becomes operational, the call recording (the audio file) will be attached to the transaction. At that point, just like all attachments, the recording will exist until the transaction purges.

Records of denied challenges are retained until the subject would reach the age of 110. All other firearm-related challenge records remain for 88 days from the completion of the challenge.

FFL records are retained indefinitely; however, ATF sends nightly updates to the FFL file. If the ATF updates indicate that the ATF has deactivated an FFL, the corresponding record in the NICS' FFL file is made inactive.

Information in the NICS Indices remains until the subject is no longer federally prohibited from possessing firearms; the expiration date of the record is reached; the NICS Section receives notice of the subject's death; the subject reaches 110 years of age or, if no DOB is given, 110 years have passed since entry into the NICS Indices; or the contributing agency removes the record from the NICS Indices.

The NICS maintains records in the VAF until the NICS Section receives notice that the subject is federally prohibited from possessing firearms; the NICS Section receives notice of the subject's death; the subject is 110 years of age or, if no DOB is given, 110 years have passed since entry into the VAF; or the subject requests removal of his/her information from the VAF.

## 3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's NIST 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

The main risk of the collection and use of the NICS information is that the operation of the NICS may inadvertently cause the creation of a firearm registry. This is mitigated by the requirement that all identifying information from approved transactions be purged from the system within 24 hours; any remaining information is then purged within 90 days so that NICS audit logs only retain the NTN and the date of the transaction. This is also enforced through integrity checks of the NICS audit logs.

Other than the above, there are three principal risks associated with NICS Section operations related to the unauthorized disclosure of PII. Those three risks are potential breaches of PII stored by the NICS through intentional unauthorized access (either directly to the NICS itself or through a POC state connection), access for an unauthorized purpose, and breach of physical security of the system.

There are two levels of system safeguards that address these risks—the CJIS Division Security Policy

and practices, and the NICS regulatory safeguards found at 28 C.F.R. § 25.8. These safeguards are combined with the NICS Audit Unit spot checks and other audit measures to ensure information in the NICS is only accessed and used for authorized purposes. The CJIS Division Security Policy provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for access to CJIS Division systems and information and is designed to protect and safeguard criminal justice information. The CJIS Division Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information. The NICS regulations specify minimum system safeguards to protect the integrity of the NICS. These safeguards address the physical security of NICS information and restrictions on the types of NICS information that can be disseminated to different types of users. *See* 28 C.F.R. § 25.8.

To ensure security policies are correctly implemented, access to the NICS requires multi-factor authentication. In addition, the NICS employs role-based access controls to ensure that individuals with access to the system access only the information they are authorized to see. For example, once logged into the NICS E-Check, FFLs can access only limited information about transactions they initiated. Likewise, individuals submitting electronic applications to the VAF have access to only their own information. Unauthorized attempts to access the NICS are addressed by ongoing system monitoring, review of daily transactions prior to purging them, and periodic audits of state system users. All FBI personnel with access to the NICS receive mandatory training on basic information assurance and the proper handling of PII. In addition, the system administrators receive privileged user training.

PII Confidentiality Risk Level:

☐ **Low** **X Moderate** ☐ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** **X No**

**If Yes, the system meets the NIST 800-59 definition of a National Security System.**

Access controls

| | |
|---|---|
| X | Access Enforcement: The system employs role-based access controls and enforcement mechanisms for PII. |
| X | Separation of Duties: Users of de-identified PII data are not also in roles that permit them to access the information needed to re-identify the records. |
| X | Least Privilege: User roles enforce the most restrictive set of rights/roles for each user group. |
| X | Remote Access: Remote access is prohibited or limited to encrypted communication channels. Remote access to the NICS for offsite work options is provided through a virtual private network |

| | |
|---|---|
| | encrypted tunnel. |
| X | User-Based Collaboration and Information Sharing: Automated mechanisms are in place for matching PII access authorizations to access restrictions, such as contractual/Memorandum of Understanding (MOU)/Memorandum of Agreement requirements. |
| | Access Control for Mobile Devices: Users accessing the NICS E-Check via the LEEP may access the portal from an internet capable device, including mobile devices. The LEEP does not ensure the security of the user device; however, traffic is scanned for malware and viruses. If a user accesses the LEEP via agency owned mobile assets/devices, the device is controlled at the agency level. The LEEP allows users to access the system from any public internet service provider or an internet capable device. |

Audit controls

| | |
|---|---|
| X | Auditable Events: Access to PII is audited for unauthorized access. A daily and weekly log review is conducted in accordance with the FBI security requirements. |
| X | Audit Review, Analysis, and Reporting: Audit records are regularly reviewed for inappropriate or unusual activity affecting PII; such activity is investigated and reported; and responsive action and appropriate mitigation is taken. |

Identification and Authentication controls

| | |
|---|---|
| X | Identification and Authentication: Users are uniquely identified and authenticated before accessing PII; remote access requires 2-factor authentication and 30-minute "time-out" functionality. This does not apply to external LEEP users of the NICS E-Check. Only internal users use 2-factor authentication. |

Media controls

| | |
|---|---|
| X | Media Access: Access to system media containing PII (CDs, USB flash drives, backup tapes) is restricted. |
| X | Media Marking: Media containing PII is labeled with distribution/handling caveats. The NICS media within FBI facilities are manually marked with SF710 "UNCLASSIFIED" stickers as needed. |
| X | Media Storage: Media containing PII is securely stored. The NICS does not include nor provide media for offsite transport or use. The NICS media is limited to media stored and secured within the FBI Data Center. |
| X | Media Transport: Media is encrypted or stored in a locked container during transport. The NICS does not include nor provide media for offsite transport or use. |
| X | Media Sanitation: Media is sanitized prior to re-use. All data is unclassified. Sanitization and destruction of physical media is coordinated with and conducted by the FBI Data Center in accordance with the FBI and FBI Data Center's sanitization policy and procedures. The NICS inherits these processes to ensure system components and media are properly sanitized and disposed prior to departing FBI facilities. |

Data Confidentiality controls (Be sure to also discuss in Section 1(f).)

| | |
|---|---|
| X | Transmission Confidentiality: Information is encrypted prior to transmission or encrypted |

| | |
|---|---|
| | transmission is used. The NICS general user interface, including the primary external-facing interfaces used for NICS transactions and reports download is protected via encryption employed by the CJIS Shared Enterprise Network (SEN) and the LEEP Portal. |
| | Protection of Information at Rest: Information stored on a secondary storage device (e.g., hard drive or backup tape) is encrypted. (**Required if the system meets the NIST 800-59 definition of a National Security System**.) The NICS is installed in and operates within the secured FBI facilities that protect the physical access to the NICS data stored at rest; however, information is not currently encrypted at rest. |

Information System Monitoring

| | |
|---|---|
| X | Information System Monitoring: Network boundaries are automatically monitored for unusual or suspicious transfers or events. The NICS network boundaries are automatically and regularly monitored for unusual or suspicious events as part of the CJIS SEN infrastructure by the CJIS Security Operations Center (SOC), FBI Enterprise SOC, and the NICS security team. |

# Section 4: Information Sharing

## 4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

| Recipient | How information will be shared | | | |
|---|---|---|---|---|
| | Case-by-case | Bulk transfer | Direct access | Other (specify) |
| Within the component | X | X | X | |
| DOJ components | X | X | X | The ATF roles allow them to query various sets of NICS data by the criteria defined by laws, regulations, and rules. The ATF accesses the NICS through the LEEP. They have a Federated ID and can only query and retrieve information they are authorized to access and have a need to know.<br><br>On a daily basis, the NICS transfers all denial transaction information to the ATF. The ATF also has access to the NICS Indices per 28 C.F.R. § 25.6 (j). |
| Federal entities | X | X | X | The NICS sends data to the ATF as noted and sends denied transaction data to the NCIC's NICS Denied Transaction File. |

| | | | | |
|---|---|---|---|---|
| | | | | The NICS also shares bulk files on the NICS Indices data with an agency containing the agency's own data for the purposes of synchronization of federal and state systems. These items represent all of the bulk transfers. The NICS is currently working on the specification for the NICS Indices Denial Notification which will be on a case-by-case basis only. The NICS will allow direct access to FFLs and agencies to their own data for the purposes of completing the NICS mission (performing a background check) or maintaining record accuracy (maintaining the NICS Indices). |
| State, local, tribal government entities | X | X | X | The NICS sends denied transaction data to the NCIC's NICS Denied Transaction File which is available to state, local, and tribal criminal justice agencies via the NCIC. The NICS also shares bulk files of NICS Indices records with an agency containing the agency's own data for the purposes of synchronization of federal and state systems. These items represent all of the bulk transfers. The NICS is currently working on the specification for the NICS Indices Denial Notification which will be on a case-by-case basis only. The NICS will allow direct access to FFLs and agencies to their own data for the purposes of completing the NICS mission (performing a background check) or maintaining record accuracy (maintaining the NICS Indices). |
| Public | | | | |
| Private sector | | | X | The FFLs have direct access to submit NICS background checks and receive a response from the |

| | | | | |
|---|---|---|---|---|
| | | | | NICS. They do not receive any criminal history information about a particular individual; they only receive proceed/deny/delay messages. |
| Foreign governments | X | | | Canada has access to the NICS Denied Transaction file in the NCIC. |
| Foreign entities | | | | |
| Other (specify): | X | | X | Individuals electronically applying for entry into the VAF can directly access information they have submitted about themselves and the status of their VAF applications.<br><br>Individuals who have challenged a NICS transaction may receive information about themselves or may designate a representative to receive information on their behalf. |

**4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]**

In order to mitigate the risk of unauthorized access, the NICS employs multifactor authentication and role-based access controls. For users within the NICS Section, each user has an established profile which provides capabilities based on the need/function of the user's assigned unit or team. Changes in a user's assigned unit or team are reflected in their profile and role-based access is adjusted accordingly. Audit logs capture which users access which information in the NICS, and all NICS users are audited. The system is physically housed in secure government facilities accessible only by authorized FBI employees and authorized contractors. Access by FFLs is limited to the ability to query the system and receive responses. In order to do so, FFLs must complete an enrollment form and create a code word. The MOUs are established for corporate access to the NICS E-Check. To access the NICS, an FFL must correctly provide their chosen code word so the NICS Section may identify that person as the user when calling for technical support. The POCs are allowed to receive the criminal

history information. Similarly, the POCs and terminal operators are required, as a condition of their access, to only allow terminal access to authorized agency employees and are also required to keep their systems in secure facilities accessible only by authorized agency personnel.

To protect against data breaches, the POCs are required to observe all procedures set forth in the CJIS Division Security Policy, including built-in controls to prevent data from being accessible to any terminals other than authorized terminals, screening the terminal operators, and restricting access to the terminals. In addition, FFLs that electronically transmit queries must pass a NICS security authentication before access takes place, and they are subject to the FBI's periodic audits.

Before an agency becomes a NICS Indices contributor, the FBI must determine the agency has relevant information to contribute. If an agency has relevant records to contribute to the NICS Indices, the agency must obtain permission from its CJIS Systems Agency (CSA)[23] to become a NICS Indices submitter. In most cases, an agency will work with the CSA to determine which method of submission (the NCIC or the LEEP) is the best method for entry. The agency must also have a valid ORI to make a NICS Indices entry. In the event an agency does not have an ORI, the CSA must request an ORI and steps are taken to validate the reason for entry and the need for the ORI prior to the CJIS Division's decision to create an ORI for the agency. The NICS Indices contributors are responsible for ensuring the accuracy and validity of the data they provide and will immediately correct any record determined to be invalid or incorrect.

Additionally, as another control to protect privacy, the FBI may only disclose relevant NICS records to persons or entities under the circumstances or for the purposes described in its System of Records Notice (SORN) and to the extent such disclosures are compatible with the purpose for which the information was collected. To combat potential breaches of PII caused by manually disseminating information (such as putting a letter into the wrong envelope), the NICS Section uses a system of "buddy-checking" whereby a supervisor or co-worker inspects envelope contents prior to sealing and dispatch. The risk of accidental disclosure of information is further reduced through management review and double checking of addressee identity prior to dissemination of the information. The creation of an electronic firearm-related challenge process and electronic VAF application process further reduces the risk of accidental dissemination of information to the wrong individual. The electronic processes require individuals to login to the system with their unique identifiers to receive information.

# Section 5: Notice, Consent, and Redress

## 5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

[23] A CSA is a duly authorized federal, state, local, tribal, territorial, or international criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the criminal justice information from various systems managed by the CJIS Division.

| | | |
|---|---|---|
| X | Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7. | |
| X | Yes, notice is provided by other means. | Specify how: The ATF Form 4473, the VAF application, the electronic firearm-related challenge submission form, the FFL Enrollment Form, and the NICS E-Check application all contain Privacy Act (e)(3) statements. |
| X | No, notice is not provided. | Specify why not: Individuals in the NICS Indices records and the SOI database are not directly notified that their information is being collected, maintained, or disseminated by the system. |

## 5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

| | | |
|---|---|---|
| X | Yes, individuals have the opportunity to decline to provide information. | Specify how: Individuals completing the ATF Form 4473 have the choice of either providing their information or not; however, if they choose not to provide the information, then they are not permitted to obtain the firearm from the FFL. Likewise, individuals providing information for firearm-related challenge purposes or for entry into the VAF can decline to provide their information. However, failure to provide information will result in the inability to process their firearm-related challenge or enter them into the VAF. |
| X | No, individuals do not have the opportunity to decline to provide information. | Specify why not: Information in the NICS Indices and the SOI database is provided by criminal justice agencies or other entities with information regarding prohibited individuals. Consequently, individuals do not have the opportunity to decline to provide this information. |

## 5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

| | | |
|---|---|---|
| X | Yes, individuals have an opportunity to consent to particular uses of the information. | Specify how: Individuals providing their information to the NICS for background checks, firearm-related challenges, and the VAF consent to the use of their information for those purposes. |

| | | |
|---|---|---|
| X | No, individuals do not have the opportunity to consent to particular uses of the information. | Specify why not: Much of the information on which the NICS relies is gathered by other government agencies as a result of criminal law enforcement activity (arrests and convictions) or involuntary civil process. |

### 5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Individuals are provided notice through the publication of the NICS SORN as well as the Brady Act and publication of NICS-related information in the C.F.R. Routine uses in the NICS SORN provide public notice that information in the NICS will be used for Brady Act purposes and, in limited circumstances, criminal justice/law enforcement purposes. Individuals are also provided with a Privacy Act notice on the ATF's Form 4473, the NICS E-Check application, and the FFL Enrollment Form regarding what information is requested and how it will be handled. Individuals are also given the opportunity to consent to whether they want to provide their information. Individuals applying for the VAF receive a Privacy Act notice on their application informing them why the information is being collected and how it will be used. Likewise, individuals submitting a firearm-related challenge through the electronic process receive a Privacy Act statement.

Information in the NICS Indices and the SOI Database is submitted by criminal justice agencies or other entities with information regarding individuals prohibited from receiving a firearm. This information is generally collected for criminal justice purposes; consequently, it is not feasible to provide individuals with the opportunity to consent to the collection or use of the information. This Privacy Impact Assessment provides notice of the types of information maintained within the NICS and the use of that information.

## Section 6: Information Security

### 6.1 Indicate all that apply.

| | |
|---|---|
| X | A security risk assessment has been conducted. |

| | |
|---|---|
| X | Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Certification & Accreditation (C&A) Activities were completed for each of the following Life Cycle Management Reviews: Preliminary Design Review, Critical Design Review, Final Design Review, Test Readiness Review, and System Acceptance Review (SAR). During the SAR, the accreditation package was submitted for an Authority to Operate (ATO) decision, ATO generated an Electronic Communication and an accreditation letter to the Department of Justice (DOJ). The NICS received a 3-year ATO on July 16, 2017. |
| X | Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:<br><br>The NICS validates and verifies the system's security posture through a set of standard security verification procedures and protocols. The list below displays these baseline security control measurements in place monitoring and securing the NICS information infrastructure:<br><br>Critical NICS controls subject to automated measurement and validation include:<br><br>• Inventory of authorized and unauthorized hardware<br>• Inventory of authorized and unauthorized software<br>• Secure configurations for hardware and software for which such configurations are available<br>• Secure configurations of network devices, such as firewalls and routers<br>• Boundary defense<br>• Maintenance and analysis of complete security audit logs<br>• Application software security<br>• Controlled use of administrative privileges<br>• Controlled access based on need to know<br>• Continuous vulnerability testing and remediation<br>• Dormant account monitoring and control<br>• Anti-malware defenses<br>• Limitation and control of ports, protocols and services<br>• Wireless device control/detection<br>• Data-leakage protection<br><br>The NICS security posture is validated at least yearly though Office of Management and Budget-300 security assessment reporting, Information Systems Security Officer (ISSO) life cycle security (LCS) testing, and independent vulnerability assessment testing/penetration testing or Security Division certification testing.<br><br>The ISSO LCS testing is conducted throughout the year in conjunction with configuration management changes. This testing is conducted using automated test tools and manual test cases which tests to DOJ and FBI policies. |
| X | The information is secured in accordance with Federal Information Security Management Act requirements. The date of the most recent C&A of the NICS is: July 16, 2017. |

| | | | |
|---|---|---|---|
| X | Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:<br><br>Auditing procedures in place include the following for the NICS:<br>• Identity of each user and device having access or attempting to access the system<br>• Time and date of access and log off<br>• Activities that might bypass, modify, and/or negate security features<br><br>All pertinent Red Hat Linux logs are captured, reviewed, and retained to include the following:<br>• System Logs<br>• Event Logs<br>• Security Logs<br>• Tripwire Reports<br><br>An overall audit plan is in place to conduct routine and random audits of the systems to include general and privileged users. Detailed audits for the systems components and devices are performed monthly. A crucial part of the overall plan is the regular examination for misuse of administrator and root accounts. There are no shared administrator accounts and all NICS accounts are monitored weekly for misuse. | | |
| X | Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act. | | |
| X | Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy. | | |
| X | The following training is required for authorized users to access or receive information in the system: | | |
| | X | General information security training—Admins, developers, testers, and some users in the NICS are required to take Privileged User training in addition to security training. | |
| | X | Training specific to the system for authorized users within the Department. | |
| | X | Training specific to the system for authorized users outside of the component. | |
| | X | Other (specify): Information Security training is required for all individuals with access to FBI systems. | |

## 6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

In addition to the above access and security controls, physical access to the NICS is limited to authorized FBI personnel and authorized contractors, and the system is housed in secure government facilities accessible only by authorized FBI employees. Access by FFLs is limited to the ability to query the system and receive responses. Similarly, the POCs and terminal operators are required, as a condition of their access, to only allow terminal access to authorized agency employees and are also required to keep their systems in secure facilities accessible only by authorized agency personnel. The FFLs, POCs, and those with access to the NICS are also provided specific training which includes rules covering the disclosure of information from the system. Access to the NICS through the NICS E-Check and the LEEP is role based which ensures that individuals only have access to the information

they are authorized to view. These controls were put in place to mitigate the risk of unauthorized access and/or disclosure of the information.

# Section 7: Privacy Act

## 7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

| | |
|---|---|
| **X** | Yes, and this system is covered by an existing system of records notice.<br><br>Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:<br><br>*National Instant Criminal Background Check System (NICS)*, **JUSTICE/FBI-018**, 63 Fed. Reg. 65223 (Nov. 25, 1998), as amended by 65 Fed. Reg. 78190 (Dec. 14, 2000), 66 Fed. Reg. 6676 (Jan. 22, 2001), 66 Fed. Reg. 8425 (Jan. 31, 2001), 66 Fed. Reg. 12959 (Mar. 1, 2001), and 82 Fed. Reg. 24147 (May 25, 2017). |
| **X** | Yes, and a system of records notice is in development. The NICS SORN is being republished in full to more clearly define the type of information collected and how that information is used. |
| | No, a system of records is not being created. |

## 7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Users generally retrieve information from the NICS by a combination of personal identifiers (e.g., name, DOB, SSN) or a unique identifier for the data they seek (e.g., NTN, FFL number, AMD number). Regardless of whether the proposed transferee is a U.S. citizen or a lawful permanent resident alien, the manner of information retrieval is the same. For more information on retrieval processes, please see Section 1.