

(h) In cases where a transfer is denied by a POC, the POC should provide a denial notification to the NICS. This denial notification will include the name of the person who was denied a firearm and the NTN. The information provided in the denial notification will be maintained in the NICS Audit Log described in § 25.9(b). This notification may be provided immediately by electronic message to the NICS (i.e., at the time the transfer is denied) or as soon thereafter as possible. If a denial notification is not provided by a POC, the NICS will assume that the transfer was allowed and will destroy its records regarding the transfer in accordance with the procedures detailed in § 25.9.

(i) *Response recording.* FFLs are required to record the system response, whether provided by the FBI NICS Operations Center or a POC, on the appropriate ATF form for audit and inspection purposes, under 27 CFR part 178 recordkeeping requirements. The FBI NICS Operations Center response will always include an NTN and associated “Proceed,” “Delayed,” or “Denied” determination. POC responses may vary as discussed in paragraph (g) of this section. In these instances, FFLs will record the POC response, including any transaction number and/or determination.

(j) *Access to the NICS Index for purposes unrelated to NICS background checks required by the Brady Act.* Access to the NICS Index for purposes unrelated to NICS background checks pursuant to 18 U.S.C. 922(t) shall be limited to uses for the purpose of:

(1) Providing information to Federal, state, or local 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; or

(2) Responding to an inquiry from the ATF in connection with a civil or criminal law enforcement activity relating to the Gun Control Act (18 U.S.C. Chapter 44) or the National Firearms Act (26 U.S.C. Chapter 53).

§ 25.7 Querying records in the system.

(a) The following search descriptors will be required in all queries of the system for purposes of a background check:

- (1) Name;
- (2) Sex;
- (3) Race;
- (4) Complete date of birth; and
- (5) State of residence.

(b) A unique numeric identifier may also be provided to search for additional records based on exact matches by the numeric identifier. Examples of unique numeric identifiers for purposes of this system are: Social Security number (to comply with Privacy Act requirements, a Social Security number will not be required by the NICS to perform any background check) and miscellaneous identifying numbers (e.g., military number or number assigned by Federal, state, or local authorities to an individual’s record). Additional identifiers that may be requested by the system after an initial query include height, weight, eye and hair color, and place of birth. At the option of the querying agency, these additional identifiers may also be included in the initial query of the system.

§ 25.8 System safeguards.

(a) Information maintained in the NICS Index is stored electronically for use in an FBI computer environment. The NICS central computer will reside inside a locked room within a secure facility. Access to the facility will be restricted to authorized personnel who have identified themselves and their need for access to a system security officer.

(b) Access to data stored in the NICS is restricted to duly authorized agencies. The security measures listed in paragraphs (c) through (f) of this section are the minimum to be adopted by all POCs and data sources having access to the NICS.

(c) State or local law enforcement agency computer centers designated by a Control Terminal Agency as POCs shall be authorized NCIC users and shall observe all procedures set forth in the NCIC Security Policy of 1992 when processing NICS background checks.

Department of Justice

§ 25.8

The responsibilities of the Control Terminal Agencies and the computer centers include the following:

(1) The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

(2) Since personnel at these computer centers can have access to data stored in the NICS, they must be screened thoroughly under the authority and supervision of a state Control Terminal Agency. This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state Control Terminal Agency. This screening will also apply to non-criminal justice maintenance or technical personnel.

(3) All visitors to these computer centers must be accompanied by staff personnel at all times.

(4) POCs utilizing a state/NCIC terminal to access the NICS must have the proper computer instructions written and other built-in controls to prevent data from being accessible to any terminals other than authorized terminals.

(5) Each state Control Terminal Agency shall build its data system around a central computer, through which each inquiry must pass for screening and verification.

(d) Authorized state agency remote terminal devices operated by POCs and having access to the NICS must meet the following requirements:

(1) POCs and data sources having terminals with access to the NICS must physically place these terminals in secure locations within the authorized agency;

(2) The agencies having terminals with access to the NICS must screen terminal operators and must restrict access to the terminals to a minimum number of authorized employees; and

(3) Copies of NICS data obtained from terminal devices must be afforded appropriate security to prevent any unauthorized access or use.

(e) FFL remote terminal devices may be used to transmit queries to the NICS via electronic dial-up access. The

following procedures will apply to such queries:

(1) The NICS will incorporate a security authentication mechanism that performs FFL dial-up user authentication before network access takes place;

(2) The proper use of dial-up circuits by FFLs will be included as part of the periodic audits by the FBI; and

(3) All failed authentications will be logged by the NICS and provided to the NICS security administrator.

(f) FFLs may use the telephone to transmit queries to the NICS, in accordance with the following procedures:

(1) FFLs may contact the NICS Operations Center during its regular business hours by a telephone number provided by the FBI;

(2) FFLs will provide the NICS Representative with their FFL Number and code word, the type of sale, and the name, sex, race, date of birth, and state of residence of the prospective buyer; and

(3) The NICS will verify the FFL Number and code word before processing the request.

(g) The following precautions will be taken to help ensure the security and privacy of NICS information when FFLs contact the NICS Operations Center:

(1) Access will be restricted to the initiation of a NICS background check in connection with the proposed transfer of a firearm.

(2) The NICS Representative will only provide a response of "Proceed" or "Delayed" (with regard to the prospective firearms transfer), and will not provide the details of any record information about the transferee. In cases where potentially disqualifying information is found in response to an FFL query, the NICS Representative will provide a "Delayed" response to the FFL. Follow-up "Proceed" or "Denied" responses will be provided by the NICS Operations Center during its regular business hours.

(3) The FBI will periodically monitor telephone inquiries to ensure proper use of the system.

(h) All transactions and messages sent and received through electronic access by POCs and FFLs will be automatically logged in the NICS Audit

Log described in § 25.9(b). Information in the NICS Audit Log will include initiation and termination messages, failed authentications, and matching records located by each search transaction.

(i) The FBI will monitor and enforce compliance by NICS users with the applicable system security requirements outlined in the NICS POC Guidelines and the NICS FFL Manual (available from the NICS Operations Center, Federal Bureau of Investigation, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306-0147).

§ 25.9 Retention and destruction of records in the system.

(a) The NICS will retain NICS Index records that indicate that receipt of a firearm by the individuals to whom the records pertain would violate Federal or state law. The NICS will retain such records indefinitely, unless they are canceled by the originating agency. In cases where a firearms disability is not permanent, e.g., a disqualifying restraining order, the NICS will automatically purge the pertinent record when it is no longer disqualifying. Unless otherwise removed, records contained in the NCIC and III files that are accessed during a background check will remain in those files in accordance with established policy.

(b) The FBI will maintain an automated NICS Audit Log of all incoming and outgoing transactions that pass through the system.

(1) The NICS Audit Log will record the following information: type of transaction (inquiry or response), line number, time, date of inquiry, header, message key, ORI, and inquiry/response data (including the name and other identifying information about the prospective transferee and the NTN). In cases of allowed transfers, all information in the NICS Audit Log related to the person or the transfer, other than the NTN assigned to the transfer and the date the number was assigned, will be destroyed after not more than 90 days after the transfer is allowed. NICS Audit Log records relating to denials will be retained for 10 years, after which time they will be transferred to a Federal Records Center for storage. The NICS will not be used to establish

any system for the registration of firearms, firearm owners, or firearm transactions or dispositions, except with respect to persons prohibited from receiving a firearm by 18 U.S.C. 922 (g) or (n) or by state law.

(2) The NICS Audit Log will be used to analyze system performance, assist users in resolving operational problems, support the appeals process, or support audits of the use of the system. Searches may be conducted on the Audit Log by time frame, i.e., by day or month, or by a particular state or agency. Information in the NICS Audit Log pertaining to allowed transfers may be accessed directly only by the FBI for the purpose of conducting audits of the use and performance of the NICS. Permissible uses include extracting and providing information from the NICS Audit Log to ATF in connection with ATF's inspections of FFL records, provided that ATF destroys the information about allowed transfers within the retention period for such information set forth in paragraph (b)(1) of this section and maintains a written record certifying the destruction. Such information, however, may be retained as long as needed to pursue cases of identified misuse of the system. The NICS, including the NICS Audit Log, may not be used by any Department, agency, officer, or employee of the United States to establish any system for the registration of firearms, firearm owners, or firearm transactions or dispositions. The NICS Audit Log will be monitored and reviewed on a regular basis to detect any possible misuse of the NICS data.

(c) The following records in the FBI-operated terminals of the NICS will be subject to the Brady Act's requirements for destruction:

(1) All inquiry and response messages (regardless of media) relating to a background check that results in an allowed transfer; and

(2) All information (regardless of media) contained in the NICS Audit Log relating to a background check that results in an allowed transfer.

(d) The following records of state and local law enforcement units serving as POCs will be subject to the Brady Act's requirements for destruction: