AUDIT OF SECURITY AND CONTROLS OVER THE NATIONAL DRIVER REGISTER

National Highway Traffic Safety Administration

Report Number: FI–2008–003
Date Issued: October 29, 2007

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Inspector General

Subject: ACTION: Audit of Security and Controls Over the National Driver Register, NHTSA
Report Number: FI–2008–003

Date: October 29, 2007

From: Rebecca C. Leng
Assistant Inspector General for Financial and Information Technology Audits

Reply to Attn. of: JA–20

To: National Highway Traffic Safety Administrator

This report presents the results of our audit of the National Driver Register (NDR) Information System administered by the National Highway Traffic Safety Administration (NHTSA) in the Department of Transportation (DOT).[1] This central register allows state department of motor vehicles (DMV) officials to exchange information on problem drivers identified in each state, such as those convicted of driving under the influence of alcohol.[2]

Annually, Congress appropriates about $4 million to support NDR operations. Part of this funding is used to cover the cost associated with housing the mainframe NDR database at a contractor site. State DMVs remotely access NDR through a network managed by the American Association of Motor Vehicle Administrators (AAMVA).[3] Through the AAMVA network, state DMVs can electronically exchange information with NDR and other states.

State DMV officials report problem drivers to NDR using personally identifiable information, such as Social Security number and the driver's name, date of birth, gender, height, weight, and eye color. When state officials process a driver's license application, they are required to check the NDR database to determine if the applicant has been identified as a problem driver in another state. If a match is

[1] Congress passed the Federal Highway Safety Act of 1960 (P.L. 86-660) to establish NDR, and the National Driver Register Act of 1982 (P.L. 97-364) to convert NDR to an electronic system. The National Driver Register Act also transferred the NDR responsibility from the Department of Commerce to DOT.

[2] A problem driver is defined as being an individual whose motor vehicle operator's license has been denied, canceled, revoked, or suspended for motor vehicle-related traffic offenses.

[3] The same AAMVA network is also used to support the Commercial Driver's License Information System (CDLIS), overseen by DOT's Federal Motor Carrier Safety Administration.

found in NDR, state officials are directed to another state DMV system for details on the traffic conviction. In 2006, more than 70 million inquiries were made for drivers' license applicants, 9 million of which were found to be problem drivers in NDR.[4]

The requirement to check applicants against NDR was intended to prevent problem drivers from "license shopping"—going to a different state to get a new driver's license when their current licenses are suspended or revoked. Keeping problem drivers off the road is critical to the Department's goal of reducing highway fatalities and injuries. For example, of the 43,000 deaths annually on U.S. roads, 17,000 are caused by alcohol-related incidents.

Other users of NDR data include Government agencies and private companies. For example, the Federal Aviation Administration, Federal Railroad Administration, and U.S. Coast Guard use NDR information to determine whether individuals are fit to occupy safety-sensitive positions, such as flying passenger aircraft or operating passenger trains or ships. Private companies in the transportation industry, such as those operating commercial motor vehicles carrying hazardous material, also request information from NDR on job applicants. In 2006, about 800,000 inquires were made by Government agencies and private companies.

Our objectives were to determine whether (1) drivers' personally identifiable information was properly secured from unauthorized access or unapproved use, (2) problem drivers were recorded in NDR in a timely manner, and (3) an adequate contingency plan existed to ensure continued services to state DMVs in the event of a disaster. This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United States and included such tests as we considered necessary to detect fraud, waste, or abuse. Details of our scope and methodology are in Exhibit A.

RESULTS IN BRIEF

Drivers' personally identifiable information was properly secured in the NDR mainframe database; however, when transmitted or stored outside the mainframe computer, it was exposed to potential unauthorized access or unapproved use. For example, sensitive information is not encrypted when transmitted between states and NDR on the AAMVA network. In addition, problem drivers were not recorded in NDR in a timely manner—millions were not recorded until at least 1 year after conviction—and incomplete or inaccurate information on Social

[4] There are more than 200 million licensed drivers in the United States, with 42 million problem drivers' records in NDR.

Security numbers and drivers' physical attributes such as height, weight, and eye color were found in NDR. Finally, the NDR contingency plan testing was too limited to ensure adequate service to state DMVs in case of an emergency.

These issues are summarized below and detailed in the finding section, beginning on page 6.

Personally identifiable information was exposed to potential unauthorized access or unapproved use. We found security weaknesses in network transmission of sensitive information, background checks on personnel given access to NDR, and record storage and mission-critical computers in the NHTSA office.

Network Transmission. Forty-two (42) million records were properly secured in the NDR mainframe database. However, they were not encrypted when transmitted between state DMVs and NDR. Thus, they were subject to potential unauthorized access during network transmission. Federal minimum security standards require the use of sophisticated encryption protection when transmitting sensitive information such as NDR records, but NHTSA does not control network transmissions between state DMVs and NDR. Instead, AAMVA is responsible for managing the network. In response to our concerns regarding the transmission of sensitive information over the network, NHTSA is developing an agreement with AAMVA to secure the sensitive data it transmits on the network.

Background Checks on Key Personnel. DOT policies require that Federal employees and contractor personnel receive the proper level of background checks before being given access to sensitive DOT systems and information. We found serious gaps in this control area. First, NHTSA employees responsible for maintaining NDR system software did not receive the higher level background checks comparable to their sensitive work. Second, AAMVA personnel working on the NDR Help Desk did not receive any background checks. Finally, NHTSA does not know whether contractor employees who control NDR mainframe data processing received proper background checks as specified in the contract. NHTSA needs to take immediate action to correct this weakness.

Record Storage and Mission-Critical Computers Used in the NHTSA Office. File cabinets used to store NDR-related records were unlocked, unattended, and exposed to unauthorized access. Computers that NHTSA staff used to access the NDR database were connected to the DOT shared network without protection. As a result, other computers on the shared network, if not properly secured, could become an entry point to gain unauthorized access to these mission-critical computers and, in turn, pose a threat to the confidentiality, integrity and availability of NDR data. NHTSA has agreed to enhance security protection in its office.

Problem drivers were not recorded in NDR in a timely manner. Deficiencies were also found in the removal of records from NDR, recording of Social Security numbers and drivers' physical attributes, and the planned NDR modernization effort. Specifically,

Timeliness of Recording Problem Driver Records. Based on our sample test, we estimate that state DMVs did not record 6 million problem driver records in NDR until at least 1 year after conviction. This delayed reporting could significantly impair other states' ability to keep problem drivers from getting a driver's license. We could not determine the timeliness of 35 percent of the sampled records due to a system design deficiency that allowed states to override the recorded entry dates in NDR. NHTSA needs to correct this system deficiency and work with state officials to improve the timeliness of recording problem drivers in NDR.

Removing Problem Drivers' Records From NDR. When traffic convictions expire, the problem driver's records are removed from NDR through interfaces with state DMV systems. However, NHTSA staff can also remove records from NDR manually. During 2006, NHTSA manually deleted about 1,000 records based on state officials' requests. We sampled 157 requests and found 11 problem driver records that were wrongfully removed from NDR while these drivers' convictions had not expired in state DMV systems. In response to our finding, state officials restored these records in NDR. Although the number of records improperly deleted is relatively small, it could have a significant impact on public safety because problem drivers could obtain valid licenses or apply for safety-sensitive positions when their records were removed from NDR. NHTSA must strengthen controls over manual removal of records from NDR.[5]

Recording Personally Identifiable Information in NDR. When searching NDR to determine whether driver's license applicants have been identified as problem drivers, state officials enter the drivers' names and dates of birth. This can result in multiple matches in the NDR database, thus requiring further identification. To identify the driver, state officials have to use other information recorded in NDR, such as height, weight, eye color, or the applicant's Social Security number or driver's license number.[6] We found, however, that close to 18 million NDR records did not have complete information on height, weight, and eye color. We also found over 161,000 duplicate Social Security numbers, each one used by more than one driver within the same state (see details in Exhibit B). We referred

---

[5] We verified that these 11 individuals did not get new personal driver's licenses from their NDR state of record or commercial driver's licenses from any state during the period when their records were removed from NDR. However, we could not determine whether any prospective employers had inquired about these individuals during this period.

[6] More than half of the records in NDR contain Social Security numbers. Providing Social Security numbers is not required for driver's license applications under the current legislation, but will become mandatory under the Real ID Act, effective in May 2008.

information regarding these duplicate Social Security numbers to the Social Security Administration. The lack of complete and accurate information on drivers' Social Security numbers and/or physical attributes made it more difficult for states' officials to identify problem drivers. NHTSA needs to strengthen system edit checks on the information submitted by state officials.

Planning NDR Modernization. The NDR system design has stayed intact since its initial installation in the early 1980s. In 2006, NHTSA began to modernize NDR by converting flat files to a relational database and replacing programs with a modern-day programming language. Although this is definitely a step in the right direction, the planned modernization effort was too limited. For example, NHTSA did not evaluate the need to include encryption or enhanced data query capabilities in the planned upgrade, even though technologies for securing and processing information requests have changed significantly since the early 1980s. NHTSA should work with state DMVs to identify upgrade needs for modernization evaluation.

NDR contingency plan testing was too limited to ensure adequate service to state DMVs in case of emergency. Contingency planning is critical to determining whether an organization can continue to perform its mission in the event of disaster. To its credit, in cooperation with AAMVA and state DMVs, NHTSA has conducted quarterly testing of the NDR contingency plan. The testing included recovering NDR system operations at an alternate site and testing the network connection between the recovery site and AAMVAnet. However, NHTSA has not tested whether the recovery system could process a similar amount of transactions as the primary system without slowing down state DMV operations. In addition, NDR's backup tapes were stored only 15 miles away from the primary processing site. In the event of a regional disaster, NHTSA could lose both the data processing center and its off-site storage location, thereby compromising NDR's operations. NHTSA should conduct capacity testing on the recovery system and select a more distant site at which to store NDR backup tapes.

We are making a series of recommendations to help NHTSA strengthen protection of sensitive NDR data and improve the efficiency of the NDR system. A complete list of our recommendations begins on page 15 of this report. In summary, we are recommending that NHTSA:

- Establish an interconnection agreement and memorandum of understanding with AAMVA that specifies the responsibilities of both organizations for the protection of NDR; encrypt data transmissions between NHTSA, the states, and NDR contractor sites; enhance background checks on personnel with access to NDR; and better protect NHTSA facilities used to manage NDR operations.

- Work with states to ensure that data on problem drivers are entered into NDR in a timely manner and with accurate personal information about the drivers, strengthen controls over manual removal of problem driver records from NDR, and evaluate other upgrade needs for the modernization effort.

- Test the transaction processing capacity of the recovery system and store back-up tapes at a more remote site.

We provided a draft of this report to NHTSA for comment on September 5, 2007, and on October 10th we received the Agency's response. NHTSA concurred or concurred in part with our recommendations and stated that many of the corrective actions needed are already in the process of being, or have already been, completed. The response further stated that comprehensive corrective action plans have already been developed for the remaining items. NHTSA's response can be found in its entirety in the Appendix.

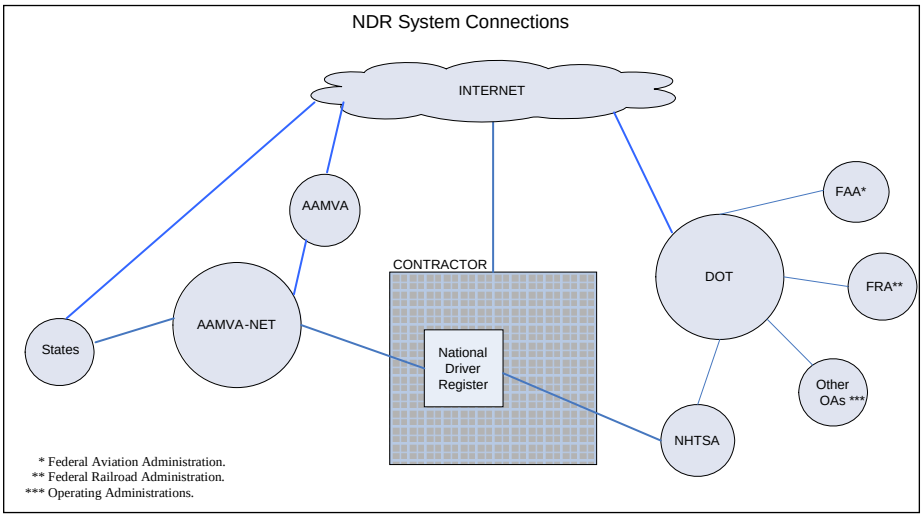
FINDINGS

Personally Identifiable Information Was Exposed to Potential Unauthorized Access or Unapproved Use

Sensitive Information Not Encrypted During Network Transmission

The NDR system resides on a mainframe computer located at a contractor's site, where 42 million driver records were properly secured. However, sensitive NDR data are not properly secured when transmitted to state DMVs via a network managed by AAMVA or to NHTSA on a dedicated line (see figure 1).

Figure 1. Overview of NDR System Network Connections



Source: DOT OIG analysis of NDR network

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the National Institute of Standards and Technology (NIST) Publication 800-53, "Recommended Security Controls for Federal Information Systems," systems that contain personally identifiable information should have their data encrypted when transmitted. Further, the Privacy Act of 1974 requires that personally identifiable information collected by the Federal Government be adequately secured to protect an individual's privacy from unauthorized access.

DOT Order H 10-202, "Departmental Guide to Network Security," requires that different organizations connecting to a DOT system develop an interconnection security agreement (ISA) and a memorandum of understanding (MOU). The ISA should document the requirements for connecting the systems and describe the security controls that will be used to protect the systems and data, along with drawings of the interconnections. The MOU should define the purpose of the interconnection, identify authorities, and specify the responsibilities of both organizations.

The states have contracted with AAMVA to provide network services to transmit and receive data to and from the NDR database. These network transmissions were not encrypted and personally identifiable information was transmitted in clear text. If intercepted during transmission, drivers' personally identifiable information could potentially be subjected to unauthorized access and unapproved use. This occurred because NHTSA did not follow departmental guidance to have an ISA and MOU with AAMVA to address security of the network connected to NDR. NHTSA should work with AAMVA to ensure that all NDR data being

transmitted at the state level are encrypted and establish an ISA and MOU with AAMVA to ensure the security of NDR data.

NHTSA also uses a dedicated line to access the NDR mainframe database; however, the data transmitted were not encrypted. NHTSA should provide data encryption for the information traversing this line.

Background Checks on Key Personnel Not Adequate

DOT Order 1630.2b, "Department of Transportation Personnel Security Manual," requires that DOT employees receive different levels of background checks in accordance with the positions they occupy. For example, employees occupying high-risk positions, especially those with significant impact on mission-critical systems, are required to receive a higher level background check (called Background Investigation). For moderate-risk positions, a lower level background check (called National Agency Check and Inquiry) is required. DOT policy also requires that contractor employees receive the same types of background checks as DOT employees who perform comparable duties.

We identified inadequate background checks for both NHTSA employees and contractor personnel.

- ***Background Checks of NHTSA Employees***. Of the 14 people responsible for monitoring and maintaining NDR system operations, 10 are NHTSA employees and 4 are contractors, all except 2 NHTSA employees received proper background checks. These two employees had the ability to make changes to NDR software, such as the criteria used to identify problem drivers, but they received only lower level background checks because NHTSA improperly assessed their positions as having a moderate risk. According to DOT policies, positions with a significant impact on mission-critical systems should be rated as having a high risk unless the work is subject to review by another position that has received the higher level background check. The two NHTSA employees' work was not subject to such a review.

- ***Background Checks of Help Desk Personnel***. Eight AAMVA personnel were responsible for operating the NDR Help Desk on behalf of NHTSA. However, none of the individuals received any background checks before potentially handling personally identifiable information as part of their duties. This happened because the cooperative agreement between NHTSA and AAMVA did not require background checks.

- ***Background Checks of NDR Contractor Personnel***. The NDR mainframe database is housed at a contractor site. In the NDR contract, NHTSA required the contractor to order background checks on personnel given access to NDR in accordance with DOT policy. However, NHTSA did not request that the contractor identify the individuals given access to NDR data or programs, nor did it specify the types of background checks required. During our visit at the contractor's site, we identified several contractor personnel with access to NDR and requested evidence of their completed background checks. Although the contractor complied with our request, we could not determine whether the background checks were adequate to meet DOT policy requirements because the contractor was unwilling to provide details on the type or level of background checks completed. As a result, there was no assurance that proper background checks had been performed on contractor personnel, who control NDR system operations, in accordance with NHTSA contract requirements.

Without proper levels of background checks, NHTSA could be missing critical information on personnel placed in key positions to ensure the integrity and security of computer operations. While background checks do not guarantee a person's loyalty or trustworthiness, they do provide valuable information with which to help management determine whether an employee should be given access to DOT systems. To mitigate the situation, NHTSA should reevaluate the position risk and associated background check requirement for the two NHTSA employees and modify the cooperative agreement with AAMVA to require AAMVA personnel providing Help Desk services to have the appropriate type of background check. In addition, it should require that the NDR data processing contractor identify individuals given access to NDR to ensure that they receive proper background checks in compliance with DOT policy.

Sensitive Records and Computers Used to Access NDR Not Properly Secured

According to NIST 800-53, only authorized users should have access to Agency information in printed or digital form. Additionally, the organization (NHTSA) should physically control and securely store information media, both physical and digital, based on the security category of information stored on the media.

At the NHTSA Headquarters NDR office, file cabinets containing personally identifiable information were unlocked—with the key in the lock during business hours. This security weakness could allow unauthorized personnel to view and obtain an individual's personally identifiable information without being noticed. According to NDR management, at least one of its personnel was physically located in the office at all times, making it unnecessary to secure doors and file cabinets during working hours. However, during two separate visits to the NDR

office, we found it unattended. NHTSA has agreed to enhance security protection in its office by keeping its NDR file cabinets locked.

Finally, we evaluated the security protection of 15 computers that NHTSA personnel use to access the NDR mainframe database. These computers reside on the network shared by thousands of DOT personnel. We found vulnerabilities in this shared network and there was no additional security protection, such as a firewall, to protect these 15 computers. Consequently, other systems/computers on the shared network could become an entry point for gaining unauthorized access to these mission-critical computers and, in turn, the NDR mainframe database. NHTSA should better protect the computers used to access the NDR mainframe database.

Problem-Driver Records Were Not Entered into NDR in a Timely Manner, Were Improperly Deleted from NDR, and Contained Incomplete and/or Inaccurate Personal Information

Problem-Driver Records Not Entered Into NDR in a Timely Manner

According to NDR, Title 49, after becoming an NDR participating state, the chief driver's licensing official of that state is responsible for submitting an individual's profile for entry into the NDR database no more than 31 days after the state DMV receives the driver's record of conviction. However, state DMVs maintain the driver's conviction date, not the date the DMV received the conviction record. According to state officials we interviewed, DMVs normally receive a driver's record about 30 days after a driver's conviction. Thus, we used the driver's conviction date plus 60 days to test the timeliness of the records entered into NDR from state DMVs.

We obtained a copy of the NDR database as of November 2005 and from that database selected a statistically valid sample of 273 records of the nine states visited. As shown in Table 1, only 100 NDR records from our sample were created within 60 days of the conviction date. In other cases, it took months or years before an NDR record was created for a driving violation. Based on the sample results, we project that records for about 6 million problem drivers were not entered into NDR until at least 1 year after conviction.[7] In addition, the timeliness of 95 sample records could not be determined because the original date of record entry was not retained in NDR—a system design deficiency.

[7] We estimate with a 90 percent confidence level that the percentage of records recorded at least 1 year after conviction is 14 percent, or about 6 million of the 42 million overall records, with a margin of error of +/- 8 percentage points.

Table 1. Timeliness Analysis of State-Sampled Records Entered into NDR

State	Number of Records	0-60 Days	61-365 Days	> 365 Days	Timeliness Cannot Be Determined
1	63	48	3	1	11
2	5	3	2	0	0
3	46	22	6	13	5
4	22	5	8	0	9
5	23	5	2	8	8
6	35	7	11	4	13
7	39	6	3	13	17
8	32	4	3	1	24
9	8	0	0	0	8
Total	**273**	**100**	**38**	**40**	**95**
		36%	**14%**	**15%**	**35%**

According to state officials we interviewed, they did not enter records of problem drivers into NDR in a timely manner partially because they were not aware of the NDR legislative requirement to send driver profile records to NDR within 31 days of the day state DMVs received them. In addition, an NDR system design deficiency caused the date of driver records' original entry to be replaced by the date that a system update occurred.

The impact of the delay in creating an NDR driver's record increases the potential that problem drivers will seek a valid license in another state before NDR is updated. To ensure the timeliness of its data, NHTSA needs to make certain that states are aware of NDR requirements for submitting the profile of convicted offenders to NDR within 31 days. Further, NDR needs to correct the system deficiency that overwrites the original record entry date so that the original dates of entry are retained.

Records of Problem Drivers Improperly Removed From NDR

Problem-driver records are deleted from NDR through system interfaces with state DMV systems when convictions expire. In addition, NHTSA personnel can manually delete records from NDR. NHTSA performed about 1,000 of these manual deletions in 2006 based on requests it received from the states. These manual deletions are done to assist the states in immediately clearing a record when a driver's license applicant has just corrected his/her status, thereby becoming eligible for a license. NHTSA requires state DMV officials to submit written requests for manual driver record deletions from NDR.

We selected two periods for review—January/February 2006 and June/July 2006. NHTSA personnel manually deleted 124 records and 33 records, respectively, during these two periods. We reviewed the written requests sent to NHTSA and found that state officials did not list justifications for the requests but used pre-authorized forms to ask NHTSA to remove records from NDR. We contacted the states and found that 11 of the 157 records we reviewed were wrongfully removed while their convictions had not expired in state DMV systems. In response to our finding, the states placed the 11 incorrectly deleted records back into NDR. We verified that none of the drivers in question received new licenses during the period that their records were incorrectly removed from NDR.

This situation existed because NHTSA did not adequately verify information on the states' request forms with designated state officials before deleting records from NDR. Additionally, they did not require state officials to provide written justification when requesting removal of a record. According to NHTSA officials, they normally verify requests with a follow-up telephone call to state officials before the record is deleted from NDR. However, they may not have done so for the 11 records that were incorrectly removed from NDR.

Finally, there was a lack of accountability—state officials could not identify the individuals who actually requested the removal of the 11 records in question. Two states, which were responsible for 9 of 11 incorrectly removed records, used pre-approved forms to request deletion of records of problem drivers from NDR. Thus, any DMV employee in these two states could ask NHTSA to remove a driver's record from NDR by using pre-approved request forms. To remediate this weakness, NHTSA should strengthen controls over the manual deletion process.

Incomplete or Inaccurate Personally Identifiable Information Impeding Identification of Problem Drivers

The National Driver Register, Title 49, requires that states send to NDR an individual's legal name, date of birth, sex, and Social Security number if states use it for driver's record or motor vehicle licensing purposes. Additionally, it requires the name of the state providing the information. The law also states that at the discretion of the Secretary of Transportation, a driver's physical attributes (height, weight, eye color) can be required as part of the NDR record to assist state DMVs in identifying the correct individual.

State officials search the NDR database for specific individuals based on last name, first initial, and date of birth.[8] Given the high number of potential matches, state officials must rely on other information recorded in NDR to identify drivers,

[8] The NDR name search algorithm uses both driver name and date of birth as the primary search factors and sex as the secondary factor in generating potential matches.

such as physical attributes or Social Security numbers. However, state DMV officials did not consistently or accurately record such identifiable information because the law does not require the information. For example, we found that drivers' physical attributes were missing from about 18 million of 42 million records in the NDR database (see details in Exhibit B). This made it more difficult for state officials to identify problem drivers. NHTSA should work with the states to determine which physical attributes are critical to identifying drivers and issue directives to mandate state submission accordingly.

Social Security numbers were included in about 26 million records (62 percent) in NDR. However, of that number, we found over 600,000 invalid Social Security numbers, such as 111-22-3333 and 222-33-4444. We also found over 161,000 duplicate Social Security numbers; that is, numbers that were used by more than one driver within the same state. This happened because state DMVs did not begin using the Social Security Online Verification System until recently. Currently, four states still do not conduct such verification.[9]

The current law does not mandate that state DMVs verify a Social Security number before issuing a driver's license. However, the Real ID Act of 2005 requires that by December 2009, all Social Security numbers used to obtain driver's licenses must be verified.[10] Until corrected, these invalid and duplicate Social Security numbers could result in confusion and impede states' ability to identify problem drivers under Real ID implementation. We provided information regarding these duplicate Social Security numbers to NHTSA and the Social Security Administration. NHTSA should work with state DMVs to correct invalid or duplicate Social Security numbers and to develop policies requiring the use of the online verification of Social Security numbers.

Modernization of NDR Too Limited

According to industry research studies, aging information systems are expensive to maintain and most are eventually retired and replaced. These studies suggest that because information systems become technically obsolete, they need to be considered for replacement every 8 to 10 years. NDR, a system that was first computerized in the early 1980s as a flat file system with COBOL programs and that uses an in-house-developed search algorithm, last underwent a system conversion in 1995. In 2005, NHTSA began to modernize NDR by converting the flat files to a relational database and replacing COBOL programs with a modern-day programming language.

---

[9] Online verification of Social Security numbers enables state officials to verify matching Social Security number, name, and date of birth of each driver through the Social Security Administration's database.

[10] The Real ID Act of 2005 establishes national standards for state-issued licenses and non-drivers' identification cards. After May 11, 2008, a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a state to any person unless the state is meeting the requirements specified in the Real ID Act.

Although this is definitely a step in the right direction, the planned modernization efforts were too limited. For example, NHTSA did not evaluate the need to upgrade NDR processing for better security protection or enhanced data integrity even though technologies for transmitting and processing information have changed significantly since the early 1980s. NHTSA should work with state DMVs to identify needed upgrades for modernization.

In addition, NHTSA did not consider replacing the in-house-developed search algorithm with commercial products (search engines). The search algorithm was developed by DOT personnel in 1982 to enable state officials to search for specific individuals in large flat files and may not be the best mechanism to search records in a relational database system. Additionally, maintaining this special search algorithm will become more expensive when the current programming staff retires. NHTSA management should evaluate whether any commercial search engine products will work more effectively with the new relational database design and improve the accuracy and response time of license applicant searches.

NDR Contingency Plan Not Adequately Tested to Ensure Sufficient Service to State DMVs in Case of Emergency

According to NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," testing is a critical element of any viable contingency plan. One area requires testing system performance using alternate equipment, another specifies that the alternate site location should be in a geographic area that is unlikely to be negatively affected by the same disaster event as the organization's primary site.

To its credit, NHTSA—in cooperation with AAMVA and state DMVs—has conducted quarterly testing of the NDR contingency plan. The exercise included recovering NDR system operations at an alternate site and testing the network connection between the recovery site and AAMVAnet. However, NHTSA has not tested whether the recovery system could process a similar number of transactions as the primary system without slowing down state DMV operations. NHTSA required only that the new telecommunications connection between AAMVAnet and the alternate NDR site be tested with a limited number of transactions. NHTSA assumed that the new telecommunications connection would provide the same level of transmission speed as the regular connection.

States have not fully participated in testing the transaction capacity of the recovery system using the new telecommunications line between AAMVA and the alternate data center. Testing would determine whether the states can use the recovery system to verify problem drivers in a timely manner and whether the new connection would result in slower processing capacity at the alternate NDR data

processing site. Either of these weaknesses could slow states' processes for issuing or renewing driver's licenses. To remediate these weaknesses, NHTSA should require states' full participation in testing the transaction processing capacity of the recovery system.

In addition, the off-site storage facility containing all NDR backup tapes is approximately 15 miles from and within the same geographic region as the primary data processing center. NIST guidelines recommend storage of backup media outside the same geographic region as the primary data center. Because of their close proximity, both facilities could be vulnerable to loss in the event of a regional disaster. According to NHTSA, these facilities were established in such close proximity by the contractor and were outside NHTSA's purview.

Loss of NDR's primary processing center and backup facility could seriously damage DOT's ability to continue operation of NDR. NHTSA management rated the system as high in its need to be available to state DMV users, because state DMVs rely on NDR to keep bad drivers from receiving licenses. Consequently, NHTSA needs to ensure that a copy of the weekly backup data files from the NDR data center is stored in a geographic region more distant than the off-site location it currently uses.

RECOMMENDATIONS

We recommend that the NHTSA Administrator direct the Senior Associate Administrator for Policy and Operations to:

Enhance security protection of NDR data by:

1. Establishing an interconnection security agreement and memorandum of understanding with AAMVA to document security requirements, identify authorities, and specify responsibilities of both organizations, such as the encryption of the data and the security assurance required to meet Government minimum security standards.

2. Installing encryption on the dedicated line between NHTSA and the NDR contractor site.

3. Requiring NDR officials to (a) re-evaluate the position risk and associated background check requirement for the two NHTSA employees with the ability to change NDR software, (b) modify the cooperative agreement to require AAMVA personnel providing Help Desk services to have the appropriate type of background check, and (c) ensure that NDR mainframe

data center employees' background checks are sufficient to meet DOT policy requirements, as specified in the contract.

4. Requiring that facilities used to store NDR records are properly secured at all times.

5. Better protecting the NHTSA computers used to access NDR mainframe database, such as installing firewall security to separate these mission-critical computers from other computers on the network.

Enhance data timeliness and accuracy by:

6. Working with states to (a) establish a mechanism to ensure that DMVs enter problem driver data into NDR within 31 days of receipt of conviction, as required by Title 49 and (b) modify the NDR database to ensure that the original date that the record of a problem driver was entered into the system is retained.

7. Requiring NDR officials to (a) develop a standard process for states to use when requesting the manual removal of problem driver records from NDR, including the driver's legal name, reason for the deletion, and name of the authorized state representative making the request and (b) require the NDR office to verify the state's request before removal of the problem driver record.

8. Requiring NDR officials to (a) work with state DMV officials to determine which physical attributes should be made mandatory for NDR reporting, provide the guidelines to the states in a directive, and establish edit checks in NDR to verify that required data fields are complete before accepting a record into the system and (b) require that state DMVs correct the invalid and duplicate Social Security numbers stored in NDR—a Federal system—and to use the online verification of Social Security numbers.

9. Requiring NDR officials to (a) work with the state DMVs to determine what functional upgrades should be included in the NDR modernization plan and (b) evaluate whether any commercially available search engine will work more effectively with the relational database design and improve the accuracy and response time of driver applicant searches.

Enhance NDR's contingency planning capability by:

10. Coordinating with state DMVs to test the transaction processing capacity of the recovery system at the contractor's alternate data center.

11. Requiring that a copy of the weekly backup data files from the NDR data center be stored in a more remote site than the one currently used.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

A draft of this report was provided to NHTSA on September 5, 2007. On October 10th we received the Agency's response, which can be found in its entirety in the Appendix. NHTSA concurred or concurred in part with our recommendations, stating that many items are already in the process of being, or have already been, completed. The response further stated that comprehensive corrective action plans have already been developed for the completion of the remaining items.

In general, the corrective actions that NHTSA management has taken and plans to take adequately address the intent of our recommendations except for recommendations 8(a), 8(b), and 10. NHTSA management's responses to our recommendations are summarized as follows:

Recommendation 1: NHTSA concurred. NHTSA is in the process of finalizing an interconnection security agreement that will include encryption of NDR data transmitted on the AAMVAnet, and a memorandum of understanding. The planned completion date for this item is December 2007.

Recommendation 2: NHTSA concurred. NDR staff and NHTSA Chief Information Officer (CIO) will work with the Department's Office of the CIO (OCIO) to establish encryption on the line between NHTSA and the contractor site where the NDR mainframe is housed. The planned completion date for this item is June 2008.

Recommendation 3 (a): NHTSA concurred. NHTSA will upgrade the position of risk designation of the employees and conduct appropriate back ground investigations. The planned completion date for this item is September 2008.

Recommendation 3 (b): NHTSA concurred. A new cooperative agreement with AAMVA will be in place in 2008 and will include a requirement for AAMVA Help Desk personnel to have appropriate background investigations according to their level of access to NDR. The planned completion date for this item is June 2008.

Recommendation 3 (c): NHTSA concurred. As part of the required annual review of security controls, NHTSA will validate the background investigations

for all employees with access to NDR. The planned completion date for this item is October 2007.

Recommendation 4: NHTSA concurred. The action required by this recommendation has been completed as of June 2007. All NDR records are currently being stored in a secure room in locked cabinets.

Recommendation 5: NHTSA concurred. The NHTSA CIO will coordinate with the Department's OCIO to obtain desktop/laptop firewall capabilities to protect the NHTSA computers used to access the NDR mainframe database. The capabilities will be tested and approved for operation in the DOT's Common Operating Environment. The planned completion date for this item is March 2008.

Recommendation 6(a): NHTSA concurred. NDR will coordinate with the state DMV's to re-emphasize the 31-day reporting requirement for revoked and suspended driver's licenses. NHTSA will post notices on the AAMVA bulletin board and advise DMV personnel of the requirement, as part of its continuing outreach initiative. The planned start date for this item is November 2007.

Recommendation 6(b): NHTSA concurred. As part of the NDR modernization effort, a field that will store the date that a pointer is first entered into the NDR is being created. The planned completion date for this item is FY 2009.

Recommendation 7(a): NHTSA concurred. A standard process used by states to request the manual removal of problem driver records from NDR has been implemented as of April 2007.

Recommendation 7(b): NHTSA concurred. NHTSA has been requiring the NDR office to verify a state's request before the manual removal of a problem driver record from the system since April 2007.

Recommendation 8(a): NHTSA concurred in part. NHTSA will consult with state DMVs to determine which physical attributes should be made mandatory for NDR reporting between November 2007 and the summer of 2008. After that, NHTSA will determine whether it should revise the reporting requirements for states' reporting to NDR. However, NHTSA does not believe that the failure to include physical attributes should be a basis for refusing a record into the NDR if other appropriate identifying information is provided.

NHTSA's proposed corrective action includes a consultation with the states to determine which physical attributes should be made mandatory for NDR reporting. However, the response goes on to state that NHTSA does not believe that the failure to include physical attributes should result in the refusal of a record

into NDR. If NHTSA intends to accept records into NDR without physical attributes, even though required, it should indicate how it intends to follow up with states to obtain the required information, such as sending a management exception report listing incomplete submissions for the states to resolve within a specified time frame. Otherwise, NHTSA's response suggests that it may establish reporting physical attributes as a requirement but will not enforce it.

Recommendation 8(b): NHTSA concurred in part. NHTSA states they will work to identify and share "best practices" for detecting duplicate SSNs contained in state DMV databases. However, since states will be required to verify SSNs under the Real ID Act, NHTSA believes that implementing a separate verification requirement would be unnecessary. The planned completion date for this item is FY 2008.

While NHTSA's proposed corrective action for verifying the SSNs of future license applicants is a step in the right direction, it did not address cleanup of invalid and duplicate SSNs already in the NDR database. Without this step, problem drivers already recorded in NDR under an inaccurate SSN could reapply for a license using the correct SSN and not be detected in NDR. The OIG provided NHTSA with a copy of duplicate and invalid SSNs that were detected in NDR. NHTSA should use this data to collaborate with the states and correct these items in NDR.

Recommendation 9(a): NHTSA concurred in part. As part of the FY 2008 alternatives analysis required for the NDR modernization capital planning process, NHTSA will initiate communications with state users to ascertain desired enhancements that should be included in the modernization process. The planned completion date for this item is September 2008. NHTSA's planned corrective action meets the intent of our recommendation.

Recommendation 9(b): NHTSA concurred. As part of the FY 2008 alternatives analysis required for the NDR modernization capital planning process, NHTSA will examine commercially available software products and determine the usefulness of incorporating them into the NDR name search algorithm. The planned completion date for this item is June 2008.

Recommendation 10: NHTSA concurred in part. NHTSA will expand the testing of the recovery system to include a more significant processing load. However, NHTSA does not believe that the disaster recovery test needs to be at normal production capacities. The planned completion date for this item is June 2008.

While increasing the volume of test data is a step in the right direction, NHTSA did not specify the transaction volume to be used in testing the recovery system. NHTSA needs to specify the planned transaction volume for testing and share the results—system response times—with state DMV users. This will help users to anticipate system performance levels in the event of an actual recovery scenario.

Recommendation 11: NHTSA concurred in part. NHTSA is currently evaluating the cost and impact of storing a copy of the weekly NDR backup tapes at a more distant alternate Federal facility. By January 2008, NHTSA will start implementing necessary changes based on the analysis results. NHTSA's planned corrective action meets the intent of our recommendation.

ACTIONS REQUIRED

Except for recommendations 8(a), 8(b), and 10, actions taken and planned by NHTSA are responsive to our recommendations and are considered resolved subject to the follow-up requirements in DOT Order 8000.1C. We would appreciate receiving NHTSA's revised response to recommendations 8a, 8b, and 10 within 30 days.

We appreciate the courtesies and cooperation of the National Highway Traffic Safety Administration during this audit. If you have any questions concerning this report, please contact me at (202) 366-1496 or Nathan Custer, Acting Program Director, at (202) 366-5540.

#

cc: Chief Information Officer, DOT
Senior Associate Administrator for Policy and Operations, NPO-010
Chief Information Officer, FMCSA
Martin Gertel, M-1
Antonyio Johnson, NPO-310

EXHIBIT A. SCOPE AND METHODOLOGY

This audit was conducted at NHTSA Headquarters in Washington, D.C.; the NDR contractor's data processing site in New Jersey; the American Association of Motor Vehicle Administrators' (AAMVA) offices in Arlington, Virginia; and the following selected state motor vehicle administration offices: California, Maryland, Nebraska, New Hampshire, New York, North Carolina, Oregon, Tennessee, and Virginia.

We reviewed NDR system security by examining policies and procedures, observing controls in operation, and conducting appropriate tests for security. We also examined the access security inherent in the NDR system and Federal, state, and contractor personnel access controls to NDR information, and used a commercial tool to assess the vulnerability of NHTSA's network.

We used a data mining tool to test the accuracy, timeliness, and completeness of the data that NDR processed. We interviewed Federal and state officials to determine the frequency of state submissions to NDR, the time it takes for NDR to update information after it is submitted, and the length of time the records are maintained in NDR. We evaluated whether verification checks were performed on specific data elements, such as Social Security numbers.

In addition, we reviewed the system's security certification documents to examine the business impact analysis and assignment of system risks, to determine whether risks had been properly assessed, and to verify whether a contingency plan existed and had been tested.

We did not test security protection of the AAMVAnet or state DMV systems because they are not NHTSA's responsibility. Our review of the Social Security numbers recorded in NDR was limited to checking for obviously incorrect and duplicate numbers. We did not validate the accuracy of Social Security numbers because all states except four were performing on-line verification with the Social Security Administration's database. We did not test whether driver's licenses were issued improperly as a result of the untimely entering of problem-driver data into NDR.

We performed our audit work between March 2005 and December 2006. This performance audit was conducted in accordance with Generally Accepted Government Auditing Standards prescribed by the Comptroller General of the United states and included such tests as we considered necessary to detect fraud, waste, and abuse.

EXHIBIT B. NDR STATE-BY-STATE DATA BREAKDOWN

State Name	Number of Records	Records Containing SSN	Duplicate SSN in-State	Records Missing Physical Attributes
Alabama	507,002	411,426	2,320	127,570
Alaska	196,344	181,261	331	22,404
Arizona	1,295,738	655,285	975	291,449
Arkansas	265,911	119,584	230	47,706
California	3,318,564	82,846	64	737,366
Colorado	1,171,788	548,469	1,237	262,557
Connecticut	329,904	176,639	67	329,904
Delaware	105,766	66,257	22	27,203
District of Columbia	74,742	59,819	44	32,549
Florida	1,929,266	1,625,678	11,214	1,929,265
Georgia	1,237,210	811,219	3,133	152,816
Hawaii	92,881	85,336	0	21,989
Idaho	233,184	189,514	3	49,373
Illinois	2,148,671	0	N/A	878,089
Indiana	783,144	574,958	2,489	117,104
Iowa	453,307	379,478	5	75,761
Kansas	391,154	267,908	933	52,423
Kentucky	349,067	328,176	93	54,149
Louisiana	443,462	375,385	14,108	9,028
Maine	356,948	137,851	1,144	147,301
Maryland	894,861	631,638	2,511	894,861
Massachusetts	1,466,277	1,101,289	7,888	1,466,277
Michigan	1,250,512	305,332	4,249	80,999
Minnesota	357,859	255,046	1,007	50,433
Mississippi	278,736	38,137	42	29,369
Missouri	741,579	671,308	16	65,649
Montana	136,991	117,618	50	10,764
Nebraska	397,253	323,703	202	64,269
Nevada	444,748	422,603	907	45,267
New Hampshire	256,102	152,537	258	103,073
New Jersey	2,277,988	1,772,504	18,890	185,339
New Mexico	281,564	274,817	193	114,337
New York	1,515,930	706,119	2,629	1,515,930
North Carolina	2,613,467	1,954,815	7,428	2,613,463
North Dakota	62,615	947	0	11,535
Ohio	1,951,414	1,856,350	0	168,148
Oklahoma	661,725	391,881	276	130,375
Oregon	1,211,533	204,901	218	1,211,533
Pennsylvania	1,641,242	1,157,012	3,046	1,641,242
Rhode Island	373,146	180,592	12,757	275,151
South Carolina	769,946	545,186	14,975	769,946
South Dakota	105,643	83,415	107	20,186
Tennessee	1,498,246	1,286,326	3,302	254,447
Texas	1,604,701	1,364,964	21,184	105,009
Utah	460,592	405,867	1,052	67,477
Vermont	183,312	117,650	982	98,318
Virginia	1,303,600	1,258,352	9,777	71,581
Washington	845,874	651,094	1,604	113,095
West Virginia	275,658	264,614	230	20,045
Wisconsin	890,268	698,513	7,134	129,761
Wyoming	83,919	75,490	53	20,961
Totals	42,521,354	26,347,709	161,379	17,714,846

N/A - Not Applicable

EXHIBIT C. MAJOR CONTRIBUTORS TO THIS REPORT

NAME	TITLE
Ed Densmore	Program Director
Nathan Custer	Project Manager
Dr. Ping Z. Sun	Project Manager
Michael P. Fruitman	Communications Adviser
Jim Mallow	Senior Auditor
Henry Lee	Computer Scientist
Mitchell Balakit	Information Technology Specialist
Christopher Cullerot	Information Technology Specialist
Vasily Gerasimov	Information Technology Specialist
Martha Morrobel	Information Technology Specialist
Harriet E. Lambert	Writer-Editor

APPENDIX. MANAGEMENT COMMENTS

Memorandum

U.S. Department
of Transportation
National Highway
Traffic Safety
Administration

Subject:	Corrective Action to Draft Report on Audit of Security and Controls Over the National Driver Register	**Date:**	October 10, 2007
From:	Nicole R. Nason Administrator X6-1836	**Reply to Attn. of:**	Rebecca Lang Office of the Inspector General X6-1488
To:	Kurt Hyde Assistant Inspector General for Surface and Maritime Programs		

Attached are the National Highway Traffic Safety Administration (NHTSA) proposed responses and corrective actions to address the eleven recommendations in the Office of the Inspector General's recent Audit of the NHTSA's Security and Controls Over the National Driver Register Program, forwarded to us on September 7.

If you have any questions on this response, please contact Antonyio Johnson, our OIG Liaison at X6- 1480.

Attachment

NHTSA
www.nhtsa.gov

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION
RESPONSE TO OIG DRAFT REPORT

TITLE: Audit of Security and Controls over the National Driver Register. **PROJECT NUMBER:** 05F3019F000.

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION POSITION

NHTSA thanks the Office of Inspector General for this report, and its willingness to work with the agency to describe most accurately the conditions surrounding the National Driver Register program. The agency's response indicates any areas where there are concerns with implementing the recommendations found in the report.

Recommendation 1: Enhance security protection of NDR data by establishing an interconnection security agreement and memorandum of understanding with AAMVA to document security requirements, identify authorities, and specify responsibilities of both organizations, such as the encryption of the data and the security assurance required to meet Government minimum security standards.

Response: Concur.

Corrective Action: NHTSA already has developed a draft interconnection security agreement and memorandum of understanding that is going through internal agency review. Once that review is completed, NHTSA will work with AAMVA to finalize and sign the recommended documents. Planned completion date: December 2007.

Recommendation 2: Enhance security protection of NDR data by installing encryption on the dedicated line between NHTSA and the NDR contractor site.

Response: Concur.

Corrective Action: NDR and NHTSA CIO will work with DOT CIO to establish encryption on the line between NHTSA and the timeshare vendor site. Planned completion date: June 2008.

Recommendation 3 (a): Enhance security protection of NDR data by requiring NDR officials to reevaluate the position risk and associated background check requirement for the two NHTSA employees with the ability to change NDR software.

Response: Concur.

Corrective Action: NHTSA will upgrade the position of risk designation of the employees and conduct appropriate background investigations. While the investigations are underway the employees will continue to function in their current duties. Reclassification of position planned completion date: September 2008.

Appendix. Management Comments

Recommendation 3 (b): Modify the cooperative agreement to require AAMVA personnel providing Help Desk services to have the appropriate type of background check.

Response: Concur.

Corrective Action: A new cooperative agreement with AAMVA will be in place in 2008 and will include a requirement for AAMVA Help Desk personnel to have an appropriate background investigation according to their level of access to the PDPS. Planned completion date: June 2008.

Recommendation 3 (c): Ensure that NDR mainframe data center employees' background checks are sufficient to meet DOT policy requirements, as specified in the contract.

Response: Concur.

Corrective Action: As part of the annual review of security controls required by NIST 800-53, NHTSA will validate the background investigations for all employees with access to the PDPS. Planned completion date: October 2007.

Recommendation 4: Require that facilities used to store NDR records are properly secured at all times

Response: Concur.

Corrective Action: The action required by this recommendation was completed in June 2007. All NDR records are now stored in a secure room in locked cabinets.

Recommendation 5: Better protecting the NHTSA computers used to access NDR mainframe database, such as installing firewall security to separate these mission critical computers from other computers on the network.

Response: Concur.

Corrective Action: NHTSA OCIO will coordinate with DOT CIO to obtain desktop/laptop firewall capabilities tested and approved for operation in the Common Operating Environment. Planned completion date: March 2008.

Recommendation 6(a): Working with the states to establish a mechanism to ensure that DMVs enter problem driver data into NDR within 31 days of receipt of conviction as required by Title 49

Response: Concur.

Corrective Action: NDR will initiate an information outreach campaign with the state DMV's to re-emphasize the need to comply with the 31-day reporting requirement for revoked and

Appendix. Management Comments

suspended driver's licenses. NHTSA will post notices on the AAMVA bulletin board and advise motor vehicle personnel of the requirement. Initial action date: Continuing outreach initiatives to commence with November 2007.

Recommendation 6(b): Working with the states to modify the NDR database to ensure that the original date that the record of a problem driver was entered into the system is retained.

Response: Concur.

Corrective Action: As part of the development of the new PDPS system, NDR is creating a field that will store the date a pointer is first entered into the PDPS. Planned completion date: FY 2009.

Recommendation 7(a): Requiring NDR officials to develop a standard process for states to use when requesting the manual removal of problem driver records from the NDR, including the driver's legal name, reason for the deletion, and name of the authorized state representative making the request.

Response: Concur.

Corrective Action: The action required by this recommendation was completed in April 2007.

Recommendation 7(b): require the NDR office to verify the state's request before removal of the problem driver record.

Response: Concur.

Corrective Action: The action required by this recommendation was completed in April 2007.

Recommendation 8(a): Requiring NDR officials to work with state DMV officials to determine which physical attributes should be made mandatory for NDR reporting, provide the guidelines to the states in a directive, and establish edit checks in the NDR to verify that required data fields are complete before accepting a record into the system.

Response: Concur-in-part.

Corrective Action: The NDR will consult with state driver licensing agencies to determine which physical attributes should be made mandatory for NDR reporting. After this consultation, the Agency will review its regulation to determine whether it is necessary to revise the current reporting requirements. However, the Agency does not believe that the failure to include physical attributes should be a basis for refusing a record into the NDR if other appropriate identifying information is provided because it may result in that record not being included in the NDR database. This in turn, may result in a revoked or suspended driver being able to obtain a driver's license in another jurisdiction. It is important to note that the Agency has limited practical ability to enforce these requirements on the states. We prefer to rely on education and

cooperation with the states to help ensure an effective NDR program. Planned completion date: Initial discussions to be held with the Motor Vehicle Administrators in November 2007 and again during the summer of 2008. Any necessary revisions to the regulation will follow these discussions.

Recommendation 8(b): require that state DMV's correct the invalid and duplicate Social Security numbers stored in NDR –a Federal system– and to use the online verification of Social Security numbers.

Response: Concur-in-part.

Corrective Action: NHTSA agrees that states should work to remove the duplicate SSN's from their licensing databases. The NDR will work with the two states that showed no duplicate Social Security Numbers to identify "best practices" for methods to detect duplicate SSN's contained on their databases. NHSTA will initiate an outreach program with the states to share these best practices. However, forty-eight states and the District of Columbia have the capability to verify the validity of SSN's with the Social Security On-Line Verification (SSOLV) system. To initiate a separate action for this recommendation for the use of SSOLV by NHTSA would be duplicative. Planned completion date: Initiate contact with two states with zero duplicate SSN's in November 2007 to document best practices. These best practices will be distributed to the states in the summer of 2008 during the AAMVA regional conferences.

Recommendation 9(a): Requiring NDR officials to work with the state DMV's to determine what functional upgrades should be included in the NDR modernization plan.

Response: Concur-in-part.

Corrective Action: As part of the FY 2008 alternatives analysis required as part of the capital planning process, the NDR will initiate communications with state users to ascertain desired enhancements and to determine whether these should result in additional system changes. Planned completion date: September 2008.

Recommendation 9(b): Evaluate whether any commercially available search engine will work more effectively with the relational database design and improve the accuracy and response time of the driver applicant searches.

Response: Concur.

Corrective Action: As part of the FY 2008 alternatives analysis required as part of the capital planning process, the NDR will examine commercially available software products to determine the usefulness of incorporating them into a future enhancement of the PDPS Name-Match database search algorithm. Planned completion date: June 2008.

Recommendation 10: Coordinating with state DMVs to test the transaction processing capacity of the recovery system at the contractor's alternate data center.

Appendix. Management Comments

Response: Concur-in-part.

Corrective Action: NHTSA will expand the recovery testing to ensure functionality with a more significant load, which should provide a closer approximation of complete system performance in times where a national emergency would require use of the recovery system. NHTSA does not believe that the disaster recovery test needs to have the backup site function at normal production capacities. Further, NIST 800-34 does not require full hot-site redundancy for systems, such as PDPS, that are not national security systems. It is neither practical nor cost effective for a state to switch their entire processing capabilities for a test of this nature. Planned completion date for expanding the recovery testing: June 2008.

Recommendation 11: Requiring a copy of the weekly backup data files from the NDR data center be stored in a more remote site than the one currently used**.**

Response: Concur-in-part.

Corrective Action: NHTSA is currently evaluating the cost and impact of storing a copy of the weekly NDR backup tapes at an alternate Federal facility. Planned completion date: Analysis by January 2008; implementing any necessary changes according to a schedule to be agreed upon with the DOT CIO following the completion of the analysis.

Appendix. Management Comments

The following pages contain textual versions of the graphs and charts found in this document. These pages were not in the original document but have been added here to accommodate assistive technology.

Security and Controls Over the National Driver Register

Section 508 Compliance Presentation

Figure 1. Overview of NDR System Connections

This diagram shows that the NDR is housed at a contractor site and how it interfaces with NHTSA at the DOT headquarters and with the States through the AAMVA network.

NHTSA is connected directly to the NDR via a dedicated line. NHTSA is also connected to the Department of Transportation's internal network, on which other DOT operating administrations also reside. Examples of these other operating administrations include the Federal Aviation Administration and the Federal Rail Administration. Every operating administration within DOT is connected to the internet via the Department's internal network.

On the State side, the NDR is directly connected to the AAMVA network. Each of the State DMVs are also connected to the AAMVA network and are able to interface with the NDR via this network. The AAMVA headquarters also is able to interface with the NDR via the AAMVA network. State DMVs and the AAMVA are connected to the internet.