INVESTIGATIVE REPORT

David Cook, Inspector General

OFFICE: INDIANA SECRETARY OF STATE
TITLE: LIMITED ACCCESS DEATH MASTER FILE ASSESSMENT AND CERTIFICATION FOR NATIONAL TECHNICAL INFORMATION SERVICE
CASE ID: 2023-06-0210
DATE: AUGUST 17, 2023

Inspector General David Cook, after review and investigation by and with OIG Director of Investigation, Mark Mitchell, issues the following report:

The mission of the Office of the Inspector General (OIG) is to investigate and prosecute fraud, waste and abuse and criminal or ethical wrongdoings in the executive branch of state government pursuant to Ind. Code §§ 4-2-7-2 and 3. The OIG also assists and aids other agencies as requested when aligned with its statutory role. Ind. Code § 4-2-7-3(1).

On June 13, 2023, the OIG received a request from the Office of the Indiana Secretary of State (SoS) asking the Inspector General (IG) to certify to the National Technical Information Service (NTIS) that the SoS systems, facilities and procedures are compliant with 15 CFR Part 1110 and PB 2016-103252, Information Security Guideline for Protection of Limited Access Death Master File (LADMF) Information (Publication 100). The certification enables the SoS to access the LADMF. The LADMF is a data base collected by the Social Security Administration identifying U.S residents who have died.

Ind. Code § 3-7-45-6.1 requires the SoS Election Division to obtain information regarding deceased voters from the Social Security Administration on at least a monthly basis. The SoS is to

compare the data collected from the LADMF to the statewide voter registration system to identify potentially deceased individuals on the voter rolls. The voter registration records that match the LADMF are shared with local county voter registration officials to (1) confirm the identified voter is, in fact, deceased, and (2) if confirmed, remove that person from the eligible voter registration list in that county. Approved state and local government officials use this information to update and ensure the accuracy of the statewide voter registration system.

To ensure the integrity of the LADMF data, the NTIS, an arm of the U.S. Department of Commerce, has created administrative regulations that require an independent accrediting body to certify that the recipient of the LADMF data has systems, facilities and procedures in place that comply with NTIS security guidelines. Pursuant to the authority of the NTIS, state or local government users of LADMF data are permitted to use the State IG to certify compliance.

NTIS has created a certification form, NTIS Form 100B, which requires the certifying party, in this case the Indiana IG, to attest to the understanding of the LADMF Certification Program Guidelines. Those guidelines include, but are not limited to, instructions for restricting access to the LADMF data, proper disposal of the restricted data, information security control requirements, physical environment protection, system and communication protection and procedures for reporting improper use and disclosure.

The IG held two meetings, one in July 2023 and the second in August 2023, attended by the Indiana IG; Special Agent Mark Mitchell; Robert Fulk, SoS CIO; Jerry Bonnet, Deputy SoS; Seth Cooper (Civix) and Sean Fahey (BakerTilly), SoS technology managers. During the meetings, the SoS through their technology management team presented information supporting the SoS attestation that their existing systems, facilities and procedures comply with security regulations

for the receipt and use of LADMF data. The SoS has attested and provided supporting information of the following:

(1) Systems: The SoS has deployed advanced information systems that meet or exceed industry standards for data security. These systems employ robust encryption, intrusions detection and prevention mechanisms to safeguard against unauthorized access data breaches and cyber threats. Stringent access controls, including multifactor authentication and role-based access, to ensure that only authorized personnel can access LADMF information are in place.

(2) Facilities: The facilities are designed with a focus on physical security. Access to LADMF information is strictly controlled and restricted to authorized personnel, electronic files are housed in a secure limited access data center. A variety of measures, including access control systems, video surveillance and alarms to ensure the integrity and security of the physical environment are employed.

(3) Procedures: The SoS has established comprehensive policies and procedures governing the handling, storage and transmission of the NTIS LADMF information. The policies are regularly reviewed and updated to align with evolving industry standards, best practices and regulatory requirements. All personnel are required to complete training on these policies and procedures to ensure continued compliance and create and maintain a culture of security awareness.

(4) Testing: The SoS conducts periodic risk assessments and vulnerability testing. Regular audits and assessments are carried out to identify and address any vulnerability or weakness in the system.

Based on the attestation by the SoS and the follow up investigation by the OIG, the IG finds that the SoS has systems, facilities and procedures in place to safeguard the LADMF information as required by 15 CFR 1110. On August 11, 2023, the IG executed the required NTIS certification form and pursuant to form instructions emailed the completed and signed NTIS Form 110 B in PDF format to NTIS. A copy of the certifications form has been sent to the SoS. Accordingly, this matter is closed.

Dated: August 17, 2023

APPROVED BY:

David Cook, Inspector General