



STATE OF ILLINOIS
**OFFICE OF THE
 AUDITOR GENERAL**

Frank J. Mautino, Auditor General

SUMMARY REPORT DIGEST

STATE BOARD OF ELECTIONS

State Compliance Examination
 For the Two Years Ended June 30, 2021

Release Date: March 17, 2022

FINDINGS THIS AUDIT: 9	AGING SCHEDULE OF REPEATED FINDINGS			
	Repeated Since	Category 1	Category 2	Category 3
Category 1:	2019	1	4, 5, 6, 7	
Category 2:	2017		2, 3,	
Category 3:				
TOTAL				

	New	Repeat	Total
Category 1:	1	1	2
Category 2:	1	6	7
Category 3:	0	0	0
TOTAL	2	7	9

FINDINGS LAST AUDIT: 8

SYNOPSIS

- (21-01) The Board did not implement adequate internal controls related to cybersecurity programs and practices.
- (21-02) The Board did not comply with certain requirements of the Election Code.
- (21-03) The Board could not demonstrate compliance with all restrictions of the Raffles and Poker Runs Act (230 ILCS 15) when granting raffle licenses.

Category 1: Findings that are **material weaknesses** in internal control and/or a **qualification** on compliance with State laws and regulations (material noncompliance).

Category 2: Findings that are **significant deficiencies** in internal control and **noncompliance** with State laws and regulations.

Category 3: Findings that have **no internal control issues but are in noncompliance** with State laws and regulations.

**STATE BOARD OF ELECTIONS
STATE COMPLIANCE EXAMINATION
For the Two Years Ended June 30, 2021**

EXPENDITURE STATISTICS (in thousands)	2021	2020	2019
Total Expenditures.....	\$ 52,712	\$ 22,118	\$ 21,075
OPERATIONS TOTAL.....	\$ 24,530	\$ 13,738	\$ 14,514
% of Total Expenditures.....	46.5%	62.1%	68.9%
Personal Services.....	5,345	5,002	4,783
Other Payroll Costs (FICA, Retirement).....	448	369	353
All Other Operating Expenditures.....	18,737	8,367	9,378
AWARDS AND GRANTS.....	\$ 28,182	\$ 8,380	\$ 6,561
% of Total Expenditures.....	53.5%	37.9%	31.1%
Total Receipts.....	\$ 8,781,997	\$ 28,986,117	\$ 1,016,359
Average Number of Employees.....	72	72	73

AGENCY DIRECTOR
During Examination Period: Steven Sandvoss (Through 06/30/21)
Currently: Bernadette Matthews

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

WEAKNESSES IN CYBERSECURITY PROGRAMS AND PRACTICES

The State Board of Elections (Board) had weak internal controls related to cybersecurity programs and practices.

The Illinois State Auditing Act (30 ILCS 5/3-2.4) requires the Auditor General to review State agencies and their cybersecurity programs and practices. During our examination of the Board's cybersecurity program, practices, and control of confidential information, we noted the Board had not:

- Developed onboarding policies.
- Developed a project management framework to ensure new applications are adequately developed and implemented in accordance with management's expectations.
- Conducted a comprehensive risk assessment or implemented risk reducing internal controls as they related to the risk assessment.
- Classified its data to identify and ensure adequate protection of information (i.e. confidential or personal information) most susceptible to attack. (Finding 1, pages 10-12)

Failure to assess and establish an adequate cybersecurity program to assess risk of confidential information being susceptible to attack

We recommended the Board develop onboarding policies, develop a project management framework to ensure new applications are adequately developed and implemented in accordance with management's expectations, conduct a comprehensive risk assessment and implement risk reducing internal controls as they related to the risk assessment, and classify its data to identify and ensure adequate protection of information (i.e. confidential or personal information) most susceptible to attack.

Board partially agreed with finding

Board officials partially agreed with the finding. The Board agreed with the first, second, and fourth bullet points. Board officials stated the Board will develop and implement an onboarding policy in accordance with the auditor's recommendations, has begun drafting policies, standards, and procedures in accordance with the auditor's recommendations, and will document the data classifications.

Board officials disagreed with the third bullet point in the finding. Board officials stated they had performed an internal Center for Internet Security (CIS) risk assessment as a gap analysis of the CIS's logical and technical controls to determine

areas of risk and provided their CIS v7.1 assessment documentation to the auditors. In addition, the Board conducted internal and third-party security assessments which included penetration testing, web application assessments, and internal security assessments. These assessments were utilized to identify weaknesses in our infrastructure, processes, procedures, documentation, and quantify risk of our agency's information systems and data. Once again, documentation of these assessments was provided to the auditors. Lastly, the Board acted to mitigate weaknesses and reduce risk identified in those assessments by implementing or strengthening internal controls. The Board will continue to conduct comprehensive security and risk assessments.

In an **accountant's comment** responding to the Board's response of the third bullet point, we agreed the Board had a third party conduct a penetration test, conduct vulnerability scans, and reviewed the CIS framework. However, a penetration test, vulnerability scans, and CIS review are only part of a comprehensive risk assessment. A comprehensive risk assessment also includes identifying the applications and confidential data in order to map the controls to safeguard the integrity, security and availability of the applications and data. The Board had not identified their applications and confidential data and associated risk reducing controls.

NONCOMPLIANCE WITH ELECTION CODE

The Board did not comply with certain requirements of the Election Code (10 ILCS 5) (Code) during the examination period.

Failure to establish monitoring of business registrations and assessing civil penalties.

As of the end of fieldwork, we noted the Board had not established monitoring mechanisms to determine whether business entities were updating their registrations as needed and, therefore, were not assessing the requisite civil penalty. Section 9-35(e) of the Code states the Board shall impose a civil penalty of \$1,000 per business day for failure to update a registration by a business entity as required by Section 20-160 of the Illinois Procurement Code (30 ILCS 500). (Finding 2, page 13)

We recommended the Board comply with the requirements of the Election Code. If the requirements of the Code require monitoring or enforcement resources beyond the present capabilities of the Board, we recommended the Board seek assistance from outside parties to perform these duties as presently prescribed in the Election Code. Otherwise, we suggested the Board seek legislative remedies from the requirements.

Board agreed with finding

Board officials agreed with this finding and stated the Board has started the process of developing a system and mechanism

to monitor and enforce these provisions of the Code, which may include seeking assistance from external resources.

NONCOMPLIANCE WITH RAFFLES AND POKER RUNS ACT

The Board could not demonstrate compliance with all restrictions of the Raffles and Poker Runs Act (Act) when granting raffle licenses.

The Act (230 ILCS 15/8.1(c)) restricts the raffle licenses issued by the Board and states the following are ineligible entities for licenses:

- i. Any political committee which has an officer who has been convicted of a felony;
- ii. Any political committee which has an officer who is or has been a professional gambler or gambling promoter;
- iii. Any political committee which has an officer who is not of good moral character;
- iv. Any political committee which has an officer who is also an officer of a firm or corporation in which a person defined in (i), (ii), (iii) has a proprietary, equitable, or credit interest, or in which such a person is active or employed;
- v. Any political committee in which a person defined in (i), (ii) or (iii) is an officer, director, or employee, whether compensated or not;
- vi. Any political committee in which a person defined in (i), (ii) or (iii) is to participate in the management or operation of a raffle as defined in this Section.

Failure to demonstrate compliance with Act

We tested 40 raffle applications received from political action committees and acted upon by the Board during the examination period. We were not able to determine whether or not the Board issued raffle licenses during the examination period to entities ineligible for licenses based upon the criteria prescribed in the Act because the Board had not established a monitoring mechanism to vet this information, therefore, no information was available to review. (Finding 3, pages 14-15)

Auditors could not determine if ineligible licenses were granted

We recommended the Board establish, implement, and document procedures for tracking and monitoring raffle licenses to ensure compliance under the Raffles and Poker Runs Act. If those specific requirements of the Act require monitoring or enforcement resources beyond the present capabilities of the Board, we recommended the Board seek assistance from outside parties to perform these duties as presently prescribed in the Act. Otherwise, we recommended

the Board continue to seek legislative remedies from the requirement.

Board agreed with the finding

Board officials agreed with this finding and stated the Board will attempt to develop a mechanism to monitor these provisions of the Code, which may include seeking assistance from external resources. In addition, Board officials stated it is currently seeking a legislative remedy.

OTHER FINDINGS

The remaining findings pertain to a failure to enter into agreement with other state agencies for the transmission of registration member data, a lack of formal change management process, inadequate disaster recovery planning, a lack of system development documentation, inadequate controls over service providers, and noncompliance with the Civil Administration Code. We will review the Board's progress towards the implementation of our recommendations in our next compliance examination.

ACCOUNTANT'S OPINION

The accountants conducted a compliance examination of the Board for the two years ended June 30, 2021, as required by the Illinois State Auditing Act. The accountants qualified their report on State compliance for Finding 2021-001 and 2021-008. Except for the noncompliance described in these findings, the accountants stated the Board complied, in all material respects, with the requirements described in the report.

The compliance examination was conducted by Sikich LLP.

SIGNED ORIGINAL ON FILE

JANE CLARK
Division Director

This report is transmitted in accordance with Section 3-14 of the Illinois State Auditing Act.

SIGNED ORIGINAL ON FILE

FRANK J. MAUTINO
Auditor General

FJM:jv