OIG CYBERSECURITY COMPLIANCE REVIEW

SUMMARY

The Broward Office of the Inspector General ("OIG") has completed a review to determine whether 23 local government entities within Broward County have complied with the Local Government Cybersecurity Act[1] ("the Act's") requirement that they adopt cybersecurity standards by January 1, 2024.

Among other things, the Act requires local governments to adopt cybersecurity standards that safeguard their data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. According to the Act, such standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity (NIST) Framework.[2]

The OIG is pleased to report that, by the time we concluded our review, all 23 local government entities had either certified to the state that they had adopted cybersecurity standards or provided us records reflecting their adoption of cybersecurity standards.

RELEVANT GOVERNING AUTHORITY

Florida Statutes

Section 282.3185 Local government cybersecurity --

(1) SHORT TITLE. – This section may be cited as the "Local Government Cybersecurity Act."

(2) DEFINITION. – As used in this section, the term "local government" means any county or municipality. . . .

(4) CYBERSECURITY STANDARDS. –

(a) Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

(b) Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each county with a

[1] Florida Statutes ("Fla. Stat.") Section ("Sec.") 282.3185 (2022).
[2] Fla. Stat. Sec. 282.3185(4)(a).

population of less than 75,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(c) Each municipality with a population of 25,000 or more must adopt the cybersecurity standards required by this subsection by January 1, 2024. Each municipality with a population of less than 25,000 must adopt the cybersecurity standards required by this subsection by January 1, 2025.

(d) Each local government shall notify the Florida Digital Service of its compliance with this subsection as soon as possible. . . .

THE OIG'S REVIEW

To enable local governments to comply with the requirement to notify the Florida Digital Service ("FDS") of their adoption of cybersecurity standards "as soon as possible," FDS made an online "Local Governance Cybersecurity Standards Attestation Form" ("Attestation Form") available through the Florida Department of Management Services, FDS web portal. (Exhibit 1[3])

The OIG sought to obtain the Attestation Forms for each local government within Broward County that was subject to meeting the Act's January 1, 2024, adoption and reporting requirements. To determine which local governments these were, the OIG obtained population estimates for Broward County and each municipality within Broward County.[4] We concluded that, as of April 1, 2023, Broward County had a population of 75,000 or more and the following municipalities had populations of 25,000 or more:

1. City of Coconut Creek
2. City of Cooper City
3. City of Coral Springs
4. City of Dania Beach
5. Town of Davie
6. City of Deerfield Beach
7. City of Fort Lauderdale
8. City of Hallandale Beach
9. City of Hollywood
10. City of Lauderdale Lakes
11. City of Lauderhill
12. City of Margate
13. City of Miramar
14. City of North Lauderdale
15. City of Oakland Park
16. City of Parkland
17. City of Pembroke Pines
18. City of Plantation
19. City of Pompano Beach
20. City of Sunrise
21. City of Tamarac
22. City of Weston

[3] This online form branches into further questions after a user answers the question, "Please indicate if your organization has adopted Cybersecurity Standards." If the user clicks on the option, "Yes," the form then populates with the additional prompts, "Adopted Cybersecurity Standards Please indicate which cybersecurity standards your organization has adopted:" and then, when that is completed, "Date of Adoption." If the user clicks on the option, "No," the form populates with the prompts, "If you have not adopted cybersecurity standards, please indicate what cybersecurity standards you will be adopting" and then "Date of when you plan to adopt." Last retrieved on August 22, 2024, from https://app.smartsheet.com/b/form/505e4dcf1d044b149d17f94b789f824c.

[4] Last retrieved on August 22, 2024, from the University of Florida, College of Liberal Arts and Sciences, Bureau of Economic and Business Research Population Program, Florida Estimates of Population 2023, at https://www.bebr.ufl.edu/wp-content/uploads/2023/12/estimates_2023.pdf.

In May 2024, the OIG issued 23 individual Letters of Request to Broward County and the above-listed 22 municipalities, seeking documents that confirmed the submission of Attestation Forms to FDS.

Responses the OIG received to those Letters of Request showed that 20 of the 23 local governments were in substantial compliance with the Act. The following three cities required additional follow-up based upon their responses.

City of Fort Lauderdale

On May 30, 2024, the City of Fort Lauderdale Clerk's Office responded to advise that there were no responsive records.

On June 6, 2024, the OIG issued a second Letter of Request to the city for "[a]ny and all policies and procedures established on cybersecurity standards as required by Section 282.3185(4)(a), Florida Statutes."

On June 18, 2024, the city Clerk's Office responded with a copy of the city's adopted cybersecurity policy dated February 1, 2024.

City of Miramar

On June 5, 2024, the City of Miramar Clerk's Office responded with a copy of its submitted Attestation Form. However, the form indicated the city had not yet adopted cybersecurity standards and planned to adopt them on March 1, 2024.

On June 6, 2024, the OIG issued a second Letter of Request to the city for "[a]ny and all records reflecting the adoption of cybersecurity standards as required by Section 282.3185(4)(a), Florida Statutes."

On June 12, 2024, the Clerk's Office responded with a copy of Resolution 24-125, "approving and adopting the National Institute of Standards and Technology's Cybersecurity Framework as the City of Miramar's Cybersecurity standards pursuant to Section 282.3185(4)(a) of the Florida Statutes." The resolution was passed and adopted on June 11, 2024, 26 days after the OIG's original request for records dated May 16, 2024.

City of Plantation

On June 3, 2024, the City of Plantation Clerk's Office responded to advise that there were no responsive records. However, also included was information from the I.T. Director advising that the city had not yet submitted the Attestation Form and was currently working on a cybersecurity policy draft that was expected to be done by the end of June 2024.

On July 2, 2024, the OIG submitted a follow-up email to inquire on the status of the cybersecurity policy draft. The response advised that the I.T. Director was completing the policy and planned to submit it for approval at the upcoming commission meeting on July 24, 2024. On July 23, 2024, the I.T. Director emailed the OIG and included a copy of the

city's submitted Attestation Form that reflected an adoption date of July 18, 2024, and a copy of the city's signed and adopted cybersecurity policy dated July 11, 2024, 51 days after the OIG's original request for records dated May 21, 2024.

In summary, 21 of the local governments the OIG reviewed responded with documentation that established they submitted Attestation Forms to the state certifying that they had adopted cybersecurity standards, and the remaining local governments, Fort Lauderdale and Miramar, provided documentation reflecting their adoption of cybersecurity standards.

During the review, the OIG noted that five cities provided documentation that established they adopted standards after the Act's deadline of January 1, 2024,[5] and three of those cities appeared to adopt standards after the OIG sent its May 2024 Letters of Request to them.[6] In addition, six cities submitted their Attestation Forms to the state after the OIG sent its May 2024 Letters of Request to those cities.[7]

CONCLUSION

Ultimately, we were pleased to conclude that, by the end of our involvement, all 23 local governments had either certified to the FDS that they had adopted cybersecurity standards or provided us records reflecting their adoption of cybersecurity standards.[8]

During the next fiscal year, we intend to conduct a similar review of the nine municipalities within Broward County with populations of less than 25,000, as the Act requires those municipalities to adopt cybersecurity standards by January 1, 2025.

The OIG appreciates the helpful cooperation of Broward County and the 22 municipalities under review in providing records and responding to inquiries.

[5] Fort Lauderdale adopted its standards on February 1, 2024, Lauderdale Lakes on May 13, 2024, Miramar on June 11, 2024, Plantation on July 11, 2024, and Pompano Beach on May 28, 2024.
[6] These were Miramar, Plantation, and Pompano Beach. See footnote 5.
[7] Coral Springs submitted its Attestation Form on May 21, 2024, Hallandale Beach on May 23, 2024, Lauderdale Lakes on May 22, 2024, Lauderhill on May 28, 2024, Plantation on July 23, 2024, and Pompano Beach on May 29, 2024. We recognize that Lauderdale Lakes had recently adopted its cybersecurity standards on May 13, 2024, prior to the OIG's Letter of Request to that city.
[8] We did not undertake to determine the substance of the Attestation Forms, that is, whether the standards these governments adopted in fact met the cybersecurity standards established by the Act.

OIG 24012-M

EXHIBIT 1

Local Governance Cybersecurity Standards Attestation Form

As required by Section 282.3185(4)(d), Florida Statutes (F.S.), each local government shall notify the Florida Digital Service of its compliance with the subsection as soon as possible.

Local Government Organizational Name: *

Please indicate the name of the local government which you are representing:

Please indicate if your organization has adopted Cybersecurity Standards. *

- ◯ Yes
- ◯ No

Cybersecurity Point of Contact

Please indicate the best point of contact for this effort:

Name: *

Title: *

Email: *

Office Phone Number: *

+1 (___) ___-____

Cell Phone Number:

+1 (___) ___-____

Acknowledgement of FS *

By checking the box on this form, you attest to the requirements set forth in Section 282.3185(4) F.S.

☐

Form Submitted by: *

(Name)

☐ Send me a copy of my responses

Submit