Public records, cybersecurity testing

Number: AGO 2019-08

Date: August 16, 2019

Subject:
Public records, cybersecurity testing

Mr. Robert A. Sugarman
Legal Counsel to the Board of Trustees, Pompano
Beach Police & Firefighters' Retirement System
100 Miracle Mile, Suite 300
Coral Gables. Florida 33134

RE: PUBLIC RECORDS – BOARD OF TRUSTEES OF THE POMPANO BEACH POLICE & FIREFIGHTERS' RETIREMENT SYSTEM – ENGAGING CYBERSECURITY VENDOR TO CONDUCT PENETRATION TESTING OF AGENCY'S ELECTRONIC DATA STORAGE SYSTEMS – whether chapter 119 precludes an agency covered by that chapter from engaging a vendor to conduct penetration testing of the agency's electronic data storage systems for the purpose of detecting and remedying vulnerabilities that would permit unauthorized persons ("hackers") to have access to information that is exempt from disclosure under sections 119.071(4)(d)2. a & d and confidential under section 119.071(4)(a)l. Sections119.071(4)(d)2. a & d and 119.071(4)(a)l, Fla. Stat.

Dear Mr. Sugarman:

This office has received your inquiry on behalf of the Board of Trustees of the Pompano Beach Police & Firefighters' Retirement System ("Trustees"), which you have described as "a local law defined benefit pension plan established by the City of Pompano Beach, Florida…to provide eligible police officers and firefighters and their survivors with retirement, death and disability benefits." Specifically, you have asked for an opinion addressing the following [rephrased] question:

Does chapter 119 preclude "an agency covered by that chapter" from engaging a "vendor to conduct penetration testing of the agency's electronic data storage systems for the purpose of detecting and remedying vulnerabilities" where such testing would potentially allow the vendor "to have access to information that is exempt from disclosure under sections 119.071(4)(d)2.a & d, Florida Statutes (2018), and confidential under section 119.071(4)(a)l., Florida Statutes" (pertaining to social security numbers)?

In sum:

If the Trustees determine that the vendor penetration testing will be "for the purpose of the administration of a pension fund" within the meaning of section 119.071(5), then it appears that any incidental disclosure to the cybersecurity vendor conducting penetration testing under a confidentiality and non-disclosure agreement would not violate chapter 119, Florida Statutes.

Additionally, potential access to or incidental release of exempt information about law enforcement personnel and firefighters to a vendor under a confidentiality agreement, for the purpose of ascertaining and ensuring its cybersecurity, would not appear to be inconsistent with the purpose underlying the exemption (i.e., ensuring the safety of such personnel), if the Trustees determine there is a “substantial policy need” to undertake the vendor penetration testing (as ultimately proposed to be implemented).

In asking this question, you have briefly described the proposed vendor services:

In order to protect the sensitive and confidential information described above and otherwise protect the integrity of [its] computer data systems, the Retirement System, at the recommendation of its computer consultant, desires to engage a third-party cybersecurity vendor to conduct penetration testing. This testing will determine the security of the information stored in the Retirement System's database. In conducting such testing, the third party will attempt to penetrate ("hack") the Retirement System's electronic data storage systems. The purpose of the penetration testing is to detect any system vulnerabilities and remedy them, thereby ensuring the safeguarding of the sensitive and confidential information. However, if the vendor is successful in penetrating the Retirement System's database security measures, the vendor will be able to inspect and copy the sensitive and confidential information protected by the statutory sections cited above. The vendor will sign a confidentiality and non-disclosure agreement. Nevertheless, the vendor will have access to this exempt and confidential information about the Retirement System's members and families.[1]

You have advised that the database is maintained by the Trustees on computers maintained by the Trustees, separate from the computer networks of the City of Pompano Beach. You have also advised the database contains personal information of current and former agency employees, including their social security numbers.

Potential Vendor Access to Social Security Numbers

As observed in your request, under section 119.071(4)(a)l, “[t]he social security numbers of all current and former agency employees which are held by the employing agency are confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.”

“If information is made confidential in the statutes, the information is not subject to inspection by the public and may only be released to the persons or organizations designated in the statute.”[2] However, section 119.071(5), Florida Statutes, provides certain exceptions to this general rule of confidentiality. As applicable here, it provides that “[s]ocial security numbers held by an agency may be disclosed if:…[t]he disclosure of the social security number is for the purpose of the administration of a pension fund administered for the agency employee's retirement fund, deferred compensation plan, or defined contribution plan.”[3]

“Administration” is defined as the “management or performance of the executive duties of a government, institution, or business; collectively, all the actions that are involved in managing the work of an organization.” Black's Law Dictionary (10th ed. 2014). While you have cited no statute addressing the proposed cybersecurity testing of the subject computer systems as applied to the Pompano Beach Police & Firefighters' Retirement System, there are statutory and rule provisions affecting state agencies and Supervisors of Elections which contemplate cybersecurity risk assessments to identify threats to information technology resources.

For example, section 282.318(4)(d), Florida Statutes—which establishes information technology services management requirements for state agencies—provides, among other things, that each "state agency head shall, at a minimum:…(d) Conduct, and update every 3 years, a comprehensive risk assessment, which may be completed by a private sector vendor, to determine the security threats to the data, information, and information technology resources, including mobile devices and print environments, of the agency. The risk assessment must comply with the risk assessment methodology developed by the Agency for State Technology[.]" Although the promulgated risk assessment regulations do not specifically mention penetration testing, they do require that state agencies "[i]dentify and document asset vulnerabilities." Fla. Admin. Code R. 74-2.002.

Further, rule 1S-2.004 of the Florida Administrative Code, which applies to Supervisors of Elections, does identify "penetration testing" as an "appropriate" security procedure. It provides that the "Supervisor of Elections or a governing body may use a certified voting system in an assessment to examine or evaluate the system's security procedures, access control, system reliability and accuracy." It also requires Supervisors of Elections to "implement appropriate procedures," which "may be conducted as a routine test, a system audit or an examination of the functionality of the software and firmware, including penetration testing." The rule also provides that, "although the Supervisor of Elections is responsible for the conduct of an assessment, he or she may use the services of an independent professional person or entity. The services of an appropriate skill assessment team who are educated and experienced in assessments and whose credentials have been approved by the governing body may be used."

Penetration testing is a "specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries."[4] Pursuant to the Federal Information Security Act, 40 U.S.C. § 1331, the National Institute for Standards and Technology ("NIST") has published standards that provide minimum information security requirements for non-defense federal information systems maintained by federal agencies.[5] These minimum security requirements include "seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored and transmitted by those systems." Id. at 2. Among those security recommendations are "access control," "audit and accountability," "certification, accreditation and security assessments," "risk assessment," and "system and information integrity." Id. at 2-3. In conjunction with federal defense and intelligence agencies, and to implement these minimum security standards, NIST has published NIST Special Publication 800-53, which sets forth information security controls. See NIST SP 800-53. Penetration testing is among the recommended controls for implementing the minimum security standards. See id. at appx. F-CA, p. F-42. Among the "control enhancements" recommended by NIST is the use of independent penetration testing agents, which are independent groups who conduct impartial penetration testing of the organization's information systems. It would thus appear that penetration testing by independent agents is a widely recognized and prudent measure to detect and remediate any vulnerabilities in government information systems.

If the Trustees determine the vendor penetration testing will be "for the purpose of the administration of a pension fund" within the meaning of section 119.071(5), then it appears that any incidental disclosure to the cybersecurity vendor conducting penetration testing under a confidentiality and non-disclosure agreement would not violate chapter 119, Florida Statutes.

Potential Vendor Access to Exempt Employee Information

Section 119.071 also provides, in subsection (4)(d)2, that the "home addresses, telephone numbers, dates of birth, and photographs of active or former sworn…law enforcement personnel" and the "home addresses, telephone numbers, dates of birth, and photographs of current or former firefighters certified in compliance with s. 633.408" are "exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution."[6] Under section 119.071(4)(d)3., Florida Statutes, an agency that is not the employer of, but is the custodian of records pertaining to, one of the persons enumerated in section 119.071(4)(d), Florida Statutes, is required to maintain such person's exemption if the person or his or her employing agency submits a written request to the custodian.[7] In your letter, you have indicated that "[t]he employing agencies of the members have submitted a written request for maintenance of the exemption under subsection 119.071(4)(d)3 of the Florida Statutes."

Notwithstanding these statutory provisions, a distinction is made between public records that are "exempt" from disclosure and records that are "confidential."[8] "If records are not confidential but are only exempt from the Public Records Act, the exemption does not prohibit the showing of such information."9 Based upon this distinction, this office has concluded that, in cases when there is a statutory or substantial policy need to disclose exempt information to a requesting agency or entity, the information may be disclosed.[10]

For example, in Florida Attorney General Opinion 96-36, the City of North Miami Police Department was interested in contracting with a company that compiled, integrated, synthesized, and summarized raw police and other data from a variety of sources and provided informational reports to law enforcement in a format that was "helpful and user friendly." As explained by the Department, it "would enter into an agreement with the entity in which the entity would agree to maintain the confidentiality of such information." The Department further indicated that it believed "that the police department's relationship with such an entity is both necessary and appropriate." Observing that the "release of exempt criminal investigative information to a company that compiles and summarizes raw police data and provides informational reports to law enforcement in a format that is helpful and user friendly" was "not inconsistent with the purpose underlying the exemption for active criminal investigative information," this office concluded "that the police department may release active criminal investigative information exempted by section 119.07(3)(b) [now 119.071(2)(c)1], Florida Statutes, to the company for the purpose of compiling, synthesizing, and summarizing such information for the police department."

As applied here, information about law enforcement personnel and firefighters is exempt from disclosure in the interest of ensuring the safety of such personnel. Potential access to or incidental release of such information to a vendor under a confidentiality agreement, for the purpose of ascertaining and ensuring its cybersecurity, would not appear to be inconsistent with the purpose underlying the exemption, if the Trustees determine there is a "substantial policy need" to undertake the vendor penetration testing (as ultimately proposed to be implemented).

Sincerely,

Ashley Moody
Attorney General

AM/tlm

[1] It is beyond the scope of this analysis to address whether the Trustees are generally authorized to enter into vendor agreements for services, and whether the procurement process, ultimate description of services, specific contract provisions addressing the security of penetration testing operations, or consideration of alternative cybersecurity assessment tools (matters this description does not disclose) might provide additional safeguards for exempt or confidential information.

[2] WFTV, Inc. v. School Bd. of Seminole, 874 So. 2d 48, 53 (Fla. 5th DCA 2004).

[3] § 119.071(5)(a)(6)(g), Fla. Stat. (2019) (emphasis added).

[4] See National Institute for Standards and Technology, Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", at appx. F-CA, p. F-62, available at http://dx.doi.org/10.6028/NIST.
SP.800-53r4 (Last Visited May 15, 2019) (hereinafter "NIST SP 800-53").

[5] See FIPS PUB 200 "Minimum Security Requirements for Federal Information and Information Systems", available at https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.
FIPS.200.pdf (Last Visited May 15, 2019).

[6] § 119.071(4)(d)2.a, d, Fla. Stat. (2019).

[7] See Ops. Att'y Gen. Fla. 14-07 (2014); 10-37 (2010); 05-38 (2005).

[8] See Rameses, Inc. v. Demings, 29 So. 3d 418, 421 (Fla. 5th DCA 2010) ("[T]he Public Records Act is construed liberally in favor of openness, and exemptions from disclosure are construed narrowly and limited to their designated purpose.").

[9] Id.

[10] See Op. Att'y Gen. Fla. 90-50 (1990); see also Inf. Op. to Hon. Don R. Amunds, Chair of Okaloosa Bd. of County Commissioners (June 8, 2012).