Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Tricia Ralph

REVIEW REPORT 22-11

May 17, 2022

Halifax Regional Police

Summary: The Halifax Regional Police (Police) underwent an audit by KPMG to evaluate the state of its information technology security. The applicant sought a copy of the KPMG audit report and any correspondence about it. The Police withheld the records in full on the basis that releasing them would harm the security of its information technology system (s. 475(1)(k) of the *Municipal Government Act*). The Commissioner finds that some of the information can be withheld under s. 475(1)(k) but she recommends the Police reconsider its application in light of the requirement to apply discretion. The Commissioner finds that releasing some of the information on portions of the responsive records could not reasonably be expected to harm the system's security and so recommends its disclosure.

INTRODUCTION:

[1] In 2016, the Halifax Regional Police (Police) underwent an audit conducted by KPMG[1] to evaluate the state of its information technology security and to set out the impact and likelihood of possible problems.[2] The applicant requested a copy of the KPMG audit report and associated correspondence:

> "A copy of KPMG's draft cyber threat assessment report on HRP's security of systems, data and policies and any correspondence related to its contents from June 2017 to January 1, 2018."

[2] The Police withheld the responsive records in full, arguing that it was authorized to withhold them because their release could reasonably be expected to harm the security of any property or system, per s. 475(1)(k) of the *Municipal Government Act* (*MGA*).

[3] The responsive records include the KPMG audit report and a two-page email.

---

[1] According to its website, KPMG is a company that offers audit, tax and advisory services. https://home.kpmg/xx/en/home/about/who-we-are.html.
[2] Zane Woodford, *New officer working to fix problematic Halifax police IT security* (September 17, 2018), online: Toronto Star https://www.thestar.com/halifax/2018/09/17/new-officer-working-to-fix-problematic-halifax-police-it-security.html?rf.

ISSUE:

[4] Was the Police authorized to refuse access to information under s. 475(1)(k) of the *MGA* because the disclosure would harm the security of any property or system?

DISCUSSION:

Burden of proof

[5] The Police bears the burden of proving that the applicant has no right of access to a record or part of a record.[3]

Was the Police authorized to refuse access to information under s. 475(1)(k) of the MGA because the disclosure would harm the security of any property or system?

[6] Section 475(1)(k) provides:

> (1) The responsible officer may refuse to disclose information to an applicant if the disclosure could reasonably be expected to
>
> (k) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[7] For the reasons set out below, I find that releasing some of the information on portions of the responsive records could not reasonably be expected to harm the system's security and so recommend its disclosure. In some cases, I find that the Police may continue to withhold information. However, I note that the Police did not demonstrate it exercised discretion and so recommend it do so and release any additional information as a result of that exercise.

[8] Section 475(1)(k) has two essential requirements. First, the Police must establish that the disclosure of the information could reasonably be expected to cause harm. Second, the harm must be to the security of any property or system.

[9] The Police has the burden of proving that this exemption applies to the records. In 2014, the Supreme Court of Canada reviewed decisions on the "reasonable expectation of harm test" contained in access to information legislation and summarized the appropriate test as follows:

> [54] This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground.[4]

---

[3] *MGA*, s. 498.

[4] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII), [2014] 1 SCR 674. Note this test was cited with approval more recently in *Houston v. Nova Scotia (Minister of Transportation and Infrastructure Renewal)*, 2021 NSSC 23 (CanLII) at paras. 64-67.

[10] The applicant provided representations setting out his position that the records should be disclosed to him. His position was that it is no secret that the Police's information technology security was endangered. He pointed me to several documents that were released after he filed his access to information request in January 2018. Specifically, he discussed the 2021 Halifax Regional Municipality's Auditor General report titled *Halifax Regional Police Information Technology Audit – Public*.[5] He acknowledged that due to the sensitive nature of information technology, many of the details of the audit were discussed in a separate, in camera report. Nevertheless, he noted that a public report was still made available and that this report detailed severe risks and urgent recommendations to improve the Police's information technology security. In his view, the same process could have been followed with the KPMG audit report, such that a similar and redacted version of it could have been released to him when he requested it in 2018. In any event, the applicant thought that the majority of the content of the KPMG audit report would likely have been brought to light by now as a result of the Auditor General's audit.

[11] The thrust of the Police's argument was that the KPMG audit report contains sufficient details that if released, could be exploited by bad actors and jeopardize the Police's cybersecurity. The Police's representations also set out some detail about the specific security risks posed by various portions of the KPMG audit report. While I disagree that the entire KPMG audit report should be withheld, in some cases I agree with the Police that some portions of it can be. Where I find that the information can be withheld, it is because the Police identified specific security risks, along with how release of that information could reasonably be expected to harm the security of the Police's cybersecurity system.

[12] That being said, s. 475(1)(k) is a discretionary exemption. Former Commissioner Tully explained the relevant factors and considerations in the exercise of discretion in *NS Review Report 18-02*,[6] which I adopt but will not repeat here. The Police provided no explanation for any factors it used in the exercise of discretion. As such, I recommend that the Police reconsider the application of s. 475(1)(k) in light of the requirement to apply discretion.

[13] The Police will be provided with an appendix to this report that sets out what portions of the KPMG audit report and two-page email I find should be released or can be withheld (following its reconsideration of discretion).

[14] Where I find that portions of the KPMG audit report and two-page email should be released, it is because the Police failed to satisfy its burden of establishing that the disclosure of the information could reasonably be expected to harm the Police's cybersecurity system. It is not enough to simply state that release of the information would harm the system and therefore it should not be disclosed. Much more is needed than that. The Police must not only set out the specific risks to the system but also connect such risks to the exact information at issue. Broad assertions of general harm are not sufficient to satisfy the burden of establishing that disclosure

---

[5] Evangeline Colman-Sadd, *Halifax Regional Police Information Technology Audit – Public* (February 4, 2021), online: https://hrmauditorgeneral.ca/themes/user/site/default/asset/img/common/Halifax_Regional_Police_Information_Technology_Audit_%E2%80%93_Public_Report_1.pdf.

[6] *NS Review Report 18-02, Department of Community Services (Re)*, 2018 NSOIPC 2 (CanLII), at paras. 45-50.

of the information could reasonably be expected to harm the security of the Police's cybersecurity system.

[15] In terms of the responsive email, the Police provided no representations on why it should be withheld. Accordingly, the Police did not meet its burden and so I cannot agree that release of the email could reasonably be expected to harm the security of the Police's cybersecurity system.

[16] I find that some but not all of the withheld information qualifies for exemption under s. 475(1)(k).

FINDINGS & RECOMMENDATIONS:

[17] I find that:

1. Section 475(1)(k) applies to some, but not all of the withheld information, as set out in the appendix provided to the Police only.
2. The Police failed to demonstrate that it exercised discretion in withholding information under s. 475(1)(k).

[18] I recommend that:

1. The Police disclose to the applicant, with a copy to the OIPC, the information withheld under s. 475(1)(k) as set out in the appendix, which has been provided to the Police only, within 45 days of the date of this review report.
2. Where s. 475(1)(k) applies, the Police reconsider its application in light of the requirement to apply discretion. Then, disclose any additional information, with a copy to the OIPC, that can now be disclosed to the applicant within 45 days of the date of this review report.

May 17, 2022

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia

OIPC File: 18-00049