Federal Court Cour fédérale

Date: 20250922

Docket: T-2284-25

Citation: 2025 FC 1527

Toronto, Ontario, September 22, 2025

PRESENT: The Honourable Madam Justice Furlanetto

BETWEEN:

HIKVISION CANADA INC. AND HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.

Applicants

and

CANADA (ATTORNEY GENERAL)

Respondent

PUBLIC ORDER AND REASONS
(Confidential Order and Reasons issued September 16, 2025)

I. Overview

[1] The Applicants, Hikvision Canada Inc [Hikvision Canada] and Hangzhou Hikvision Digital Technology Co Ltd [Hikvision], seek to stay an Order of the Governor in Council [GIC], dated June 27, 2025 [OIC], made pursuant to subsection 25.4(1) of the *Investment Canada Act*, R.S.C. 1985, c 28 [ICA], until the disposition of the underlying judicial review proceeding or a

date to be fixed by the Court. The OIC required Hikvision Canada to windup its business and cease all operations in Canada within 120 days on the basis that it [the Investment] was injurious to national security.

[2] To stay the application, the Applicants must satisfy the three-part test set out in *RJR-MacDonald Inc v Canada (Attorney General)*, [1994] 1 SCR 311 at 334 [*RJR*], namely that: (i) there is a serious issue to be tried; (ii) they will suffer irreparable harm if the stay is not granted; and (iii) the balance of convenience favours granting a stay because they will suffer greater harm if the stay is not granted than the Respondent, Attorney General of Canada [AGC], will suffer if the stay is granted.

[3] The AGC concedes there is a serious issue to be tried and that Hikvision Canada will suffer some irreparable harm if the stay is not granted but does not agree that the balance of convenience lies in the Applicants' favour. For the reasons set out further below, it is my view that the increased risk to the public that will arise as a matter of national security from the proliferation of product by Hikvision Canada if the stay is granted outweighs the commercial harms to the Applicants if the stay is not imposed. As such, the motion will be dismissed. However, I will order the application to proceed to case management so that a hearing date and timetable for the remaining steps in the application can be scheduled expeditiously.

II. **Background**

A. *Legislative Scheme under the ICA*

[4] The ICA is the primary mechanism for the Government of Canada to review foreign investments in Canada. One of the purposes of the ICA is to provide for a review of significant investments in Canada by non-Canadians that could be injurious to national security. Such an investment, as in this case, can be a "new Canadian business".

[5] Pursuant to subsection 11(a) and section 12 of the ICA, a non-Canadian making an investment to establish a new Canadian business must file a notification with the Director of Investments [Director] prior to implementation of the investment or within thirty days thereafter. Upon receipt of the notification and certification of its date, the Minister of Industry [Minister] has forty-five days to determine whether there are reasonable grounds to believe that the investment could be injurious to national security (subsection 25.2(1) of the ICA). The review process is conducted by the Investment Review Directorate [IRD] of the Foreign Investment Review and Economic Security [FIRES] Branch of Innovation, Science and Economic Development Canada [ISED] with support from the Minister of Public Safety and Emergency Preparedness [MPSEP] and other government departments and agencies, including the Canadian Security Intelligence Service [CSIS], the Communications Security Establishment and the Department of National Defence.

[6] Where the Minister determines that an investment could be injurious to national security, it is required to make an order for further review of the investment (subsection 25.3(1) of the ICA). Where further review is conducted, the non-Canadian entity is entitled to make

representations and to submit written undertakings in response to the notice (subsection 25.3(4) of the ICA). The non-Canadian entity will also receive a summary of the Minister's concerns. Only after consideration of these materials, further consultation with the MPSEP and others, and a report by the Minister with recommendations will the investment be referred to the GIC for further order.

[7] Once referred, the GIC may by order take any measures that it considers advisable to protect national security, including (a) directing the non-Canadian not to implement the investment; (b) authorizing the non-Canadian to make the investment on the terms and conditions contained in the order; or (c) requiring the non-Canadian to divest themselves of control of the Canadian business or of their investment in the entity (subsection 25.4(1) of the ICA). An order by the GIC is final and cannot be appealed but is subject to judicial review under the *Federal Courts Act*, RSC, 1985, c F-7 (section 25.6 of the ICA).

B. *National Security Review of Hikvision Canada*

[8] The Investment, Hikvision Canada, commenced its operations in Canada in May 2015. Hikvision Canada is a wholly owned subsidiary of HDT International Limited, a Hong Kong corporation, which through direct and indirect holdings is wholly owned by Hikvision, a public company listed on the Shenzhen Stock Exchange, with its country of origin in the People's Republic of China [PRC]. As of the date of the OIC, the State-Owned Assets and Supervision and Administration Commission of China, a PRC government entity, indirectly owned 41.12% voting interest and the greatest share of Hikvision through three wholly owned subsidiary entities within the China Electronics Technology Group [CETC].

[9] Hikvision Canada is engaged in the sale and distribution of Internet of Things (or “IoT”) products, including security cameras, network video recorders, access control systems, intercoms, corresponding device management software and conference tablets, along with traditional electronic related products including LED displays, monitors, switches and related accessories. Hikvision Canada distributes Hikvision products through third-party, independently owned, national and regional distributors who supply products to integrators and installers that then sell to end users.

[10] In September 2024, ISED contacted Hikvision Canada because it had not provided a notification under subsection 11(a) and section 12 of the ICA.

[11] On November 8, 2024, Hikvision Canada submitted its ICA notification along with a letter setting out the details of its business. The letter stated that Hikvision was late in filing the notice because it misunderstood its obligations under the ICA. The Director certified the date on which Hikvision Canada completed its notice on November 15, 2024.

[12] Between November 2024 and June 2025, a national security review was conducted on the Investment. The review included multiple Requests for Information from FIRES, responses and undertakings from Hikvision Canada, as well as an in-person presentation by Hikvision Canada to FIRES on March 6, 2025 to formally address FIRES’ summary of national security concerns.

[13] The summary of concerns included concerns that:

> Hikvision Canada Inc. (Hikvision Canada) is a subsidiary of Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision). Headquartered in Hangzhou, People's Republic of China (PRC). Hikvision has extensive links to the PRC state and the Chinese Communist Party, including through its controlling shareholder, China Electronics Technology HIK Group Co. Ltd.
>
> Hikvision is subject to the policies and laws of its national government, including the 2015 National Security Law and the 2017 Intelligence Law. These laws compel citizens and organizations to assist the organs of the PRC state, including its security and intelligence services. PRC legislative frameworks and Hikvision's relationship with the PRC government render its technology and data, wherever located and collected, vulnerable to exploitation by the PRC state.
>
> Hikvision Canada was established to facilitate the sale and distribution of Hikvision's products in Canada, through its distributor network. Its main product lines in Canada are security cameras, network video recorders, access control systems, intercoms, conference tablets, among others.
>
> The establishment and continued operation of the Canadian business for the purposes described above would result in an expanded and sustained market penetration of Hikvision products, thereby exacerbating the associated risk of PRC espionage and other intelligence activities within Canada. As such, this investment could be injurious to Canada's national security.
>
> [footnotes removed]

[14] On June 27, 2025, the GIC issued the OIC requiring, among other things, that Hikvision Canada:

> 2. ... immediately cease all operations in Canada, including by cancelling all sales orders and terminating any marketing and after-sales support services, except as necessary to meet the requirements set out in section 3.
>
> 3. Not later than 120 days after the day on which this Order is made, ...wind up its business in Canada, including by closing any place of operations in Canada, by terminating the employment of all individuals in Canada who are employed in connection with its

> operations and by terminating all contracts with individuals in Canada who are self-employed in connection with its operations.
>
> 4. In complying with the requirements set out in section 3, ... not sell or transfer any of the products it offered in Canada to entities carrying out operations in Canada.
>
> 5. ...not, directly or indirectly, carry out any part of the activities of Hikvision Canada in Canada except as necessary to meet the requirements set out in section 3.

[15] On the same day, the Minister also issued a public statement announcing the OIC, and stating that:

> ... the Government of Canada is prohibiting the purchase or use of Hikvision products in government departments, agencies and crown corporations. The Government of Canada is further conducting a review of existing properties to ensure legacy Hikvision products are not used going forward.

[16] On July 4, 2025, Hikvision Canada informed the AGC that it intended to commence an application for judicial review of the OIC and to file an urgent motion for an interim and/or interlocutory stay of the OIC.

[17] On July 5, 2025, by agreement with the AGC, the deadlines under the OIC were extended from July 4, 2025 until the date of the decision on this motion, and Hikvision Canada was permitted to resume operations in Canada [Extension Agreement].

[18] An application for judicial review was filed by Hikvision Canada on July 7, 2025. On August 31, 2025, Hikvision Canada served its evidence in the application. Hikvision Canada advises that it does not intend to bring any procedural motions. A date has not yet been set for the hearing of the application nor a timetable for next steps.

[19] The Applicant provided notice of the present motion on July 10, 2025, along with a timetable that was agreed to by the parties for filing materials and for hearing the motion.

[20] Each party filed evidence as part of their motion materials. The Applicants submitted three affidavits: two affidavits from Yang (Nicolas) Zhang, the President of Hikvision Canada, and an affidavit from Chuck Davis, Vice President of Global Information Security at Hikvision. The Zhang and Davis affidavits provide background on the Applicants and their business operations and speak to the issue of irreparable harm. The Respondent submitted a single affidavit from Robert McCarty, a Senior Investment Officer in the IRD within FIRES who was involved in the national security review of Hikvision Canada. His affidavit provides background on the ICA national review process and on the national security review of Hikvision Canada.

III. **Analysis**

[21] The sole issue before the Court on this motion is whether a stay pursuant to section 18.2 of the *Federal Courts Act*, RSC, 1985, c F-7 should be granted. This requires that the three-part test set out in *RJR* be met and, as an overarching principle, that the Court be satisfied that a stay is "just and equitable in all of the circumstances of the case": *Google Inc v Equustek Solutions Inc*, 2017 SCC 34 at paras 1 and 25.

A. *Serious Issue*

[22] As set out earlier, the first branch of the *RJR* test requires the Applicants to establish that there is a serious issue to be tried in the underlying application. The threshold for establishing a

serious issue is low and requires that the Court conduct only a preliminary assessment of the merits of the case to be satisfied that it is neither frivolous nor vexatious: *RJR* at 337-338.

[23] The Applicants argue that the judicial review application raises important issues, including the reasonableness of the OIC and whether the OIC was based on erroneous findings of fact. They argue that the national security risks upon which the OIC is premised are based on a misunderstanding about the technological features and operation of the Applicants' product. The Respondent concedes that the impugned reasonableness of the OIC is neither a frivolous nor vexatious issue. I agree that there is a serious issue to be tried such that the first part of the *RJR* test is met.

B. *Irreparable Harm*

[24] The second branch of the *RJR* test requires the Applicants to establish that they will suffer irreparable harm if a stay is not granted. As explained in *RJR* at page 341: "Irreparable harm refers to the nature of the harm suffered rather than its magnitude. It is harm which either cannot be quantified in monetary terms or which cannot be cured". Irreparable harm can include instances where one party will be put out of business by the court's decision or will suffer permanent market loss or irrevocable damage to its business reputation.

[25] To establish irreparable harm, an applicant must provide clear and non-speculative evidence that irreparable harm will occur if the stay requested is not granted: *United States Steel Corporation v Canada (Attorney General)*, 2010 FCA 200 at para 7 [*US Steel*]. The harm must be real, definite and unavoidable; not hypothetical and speculative, nor harm that can be repaired

later: *China Mobile Communications Group Co Ltd v Canada (Attorney General)*, 2021 FC 1277 at para 40 [*China Mobile*], citing *Janssen Inc v Abbvie Corporation*, 2014 FCA 112 at para 24 and *Western Oilfield Equipment Rentals Ltd v M-I LLC*, 2020 FCA 3 at para 11.

[26] On this motion, the Applicants have provided evidence on irreparable harm from both Hikvision Canada and Hikvision. In that evidence, Mr. Zhang states that the following harm will result from the OIC requiring Hikvision Canada to immediately cease operations:

- Hikvision Canada will lose sales revenue ([redacted]) that it will be unable to recover.

- Hikvision Canada will be shut out of the Canadian market by having to cancel existing orders with distributors and stop future orders, thereby prohibiting distributors from fulfilling their contractual obligations to dealer partners who in turn have obligations to their end users.

- After sales, technical and warranty support will be removed, rendering Hikvision Canada's products commercially unsupported.

- Cybersecurity support and vulnerability management to ensure the security of products will be removed. This harm is also discussed by Mr. Davis who states that this removal will leave Canadian end users vulnerable and will undermine the guidance and recommendations of the Canadian Centre for Cyber Security.

- All activities of Hikvision Canada will be stopped, including access to the Hikvision application to support Canadian end users, making the product less desirable.

[27] Mr. Zhang also refers to harm resulting from the OIC's requirement for Hikvision Canada to wind-up its business within 120 days. This harm includes the loss of up to 66 employee jobs and related expenses from the forced termination of employment without cause, penalties from leases, damage to reputation, and irrecoverable financial loss to Hikvision Canada and to third parties from the termination of service contracts and the cancellation of sales orders.

[28] While the AGC contests certain aspects of the evidence submitted, including the extent of damage asserted, it acknowledges that the second branch of the RJR test is about the nature of the harm that will be suffered and not the extent of harm. It does not dispute that there will be at least some irreparable harm to Hikvision Canada from the OIC as a result of it needing to cease its operations and wind-up its business. I agree that there will be irreparable harm and as such, that the second branch of the *RJR* test has been met. The extent of irreparable harm will be addressed when considering the balance of convenience.

C. *Balance of Convenience*

[29] The heart of the debate between the parties as it relates to the requested stay turns on the balance of convenience − that is, which party will suffer more harm with respect to the outcome of this motion and the determination of whether a stay should be granted. In view of the OIC, this necessitates consideration of the public interest.

(1) Presumption of irreparable harm to the public

[30] As a preliminary matter, the Respondent asserts that as a public authority enforcing the ICA, the nature of the OIC assumes that there is irreparable harm to the public which should weigh heavily in the balance of convenience analysis. They refer to the statement of legal principles set out by Chief Justice Paul Crampton in *China Mobile* at paragraph 51:

> [51] Where a public authority is enforcing validly enacted legislation, "the court should in most cases assume that irreparable harm to the public interest would result from the restraint of that action": *RJR*, above, at 346. Moreover, that harm often will weigh heavily in the balance: *Glooscap Heritage Society v Canada (National Revenue)*, 2012 FCA 255 at para 52. This includes where the stay sought will effectively suspend the application of the ICA to the party seeking the stay: *US Steel*, above, at para 23.

[31] The Applicants acknowledge that the ICA has a valid public purpose that ought to be given significant weight when considering the balance of convenience; however, they argue that the weight ascribed to the public interest depends on the breadth of the stay sought. The Applicants assert that where the stay sought relates to an order against an individual corporation, the public interest the Respondent claims should not dominate the analysis.

[32] The Applicants rely on the following passage from *RJR* at page 346. However, I do not agree that *Manitoba (AG) v Metropolitan Stores Ltd*, 1987 CanLII 79 (SCC) [*Metropolitan Stores*] (referenced within this passage from *RJR*) provides a parallel to the order and facts at issue here:

> Consideration of the public interest may also be influenced by other factors. In *Metropolitan Stores*, it was observed that public interest considerations will weigh more heavily in a "suspension" case than in an "exemption" case. <u>The reason for this is that the public interest is much less likely to be detrimentally affected</u>

> when a discrete and limited number of applicants are exempted from the application of certain provisions of a law than when the application of the law is suspended entirely.
>
> [Emphasis added by the Applicants]

[33] As noted by the Respondent, neither *Metropolitan Stores* nor any of the other cases cited by the Applicants (*143471 Canada Inc v Quebec (Attorney General)*, 1994 CanLII 89 (SCC); *Robinson v Canada (Attorney General)*, 2019 FC 876; *Power Workers' Union v Canada (Attorney General)*, 2022 FC 73) relate to the ICA or national security. In *US Steel*, the Federal Court of Appeal recognized that the ICA is aimed at ensuring that proposed investments will not be injurious to national security, which is a public interest focus that weighs heavily in the balance. This same principle was reiterated in *China Mobile* at paragraph 87:

> [87] ... One of the purposes of the ICA is to provide for the review of investments in Canada by non-Canadians that could be injurious to national security: ICA, s. 2. This provides a sufficient basis upon which to conclude that the ICA "is directed to the public good and services a valid public purpose": *US Steel*, above, at para 23. It is also sufficient to trigger the principle that actions taken to enforce the ICA ought to weigh heavily in the balance: *US Steel*, above, at para 23.

[34] While I agree that the Court must look at the specific harm the OIC targets, this does not take away from the fact that the ICA and the OIC deals with matters of national security which raises serious public interest concerns.

(2) The national security concerns

[35] The Applicants assert that the AGC raises three national security concerns – first, that Hikvision Canada's products will lead to unauthorized data collection; second, that Hikvision Canada is subject to foreign PRC government influence; and third, that there is a risk of

counterintelligence operations. The Applicants argue that each of these concerns are rebutted by the evidence filed on the motion.

[36] The Applicants refer to the affidavits from Mr. Zhang and Mr. Davis which state that neither Hikvision nor Hikvision Canada have access to user devices or data because Hikvision Canada does not sell products directly to end users. Instead Hikvision Canada uses authorized distributors who provide technical support through independent dealers. The evidence from Mr. Davis is that Canadian end users' audio and video information is fully encrypted and is not stored on Hikvision's cloud servers and that Hikvision devices are designed to operate with full functionality without internet access. Mr. Zhang states that Hikvision Canada is not subject to PRC law and that Hikvision Canada has never received a request to provide end user data to any foreign government and if they did, they would have no legal or factual basis to comply. Mr. Davis states that Hikvision and Hikvision Canada follow global processes regarding cybersecurity and vulnerability reporting and do not share information on vulnerabilities with other entities or government for nefarious purposes.

[37] The Applicants assert that this direct evidence rebuts the national security concerns and should be weighed more favourably than the evidence of the Respondent, which includes only third-party reports. They assert that the third-party reports make unsubstantiated claims regarding the weaponization of software vulnerabilities and provide no direct evidence that Hikvision or Hikvision Canada is assisting the PRC government or is involved in any intelligence or cyber operations by the PRC government.

[38] I agree that the harms alleged by the parties must be considered as part of the balancing exercise. However, as noted by the AGC, representations in-line with the Applicants' evidence were already evaluated in the national security review. It is not the appropriate role for the Court on this motion to reassess the merits of the OIC.

[39] As emphasized in *China Mobile,* at paragraph 100:

> [100] It bears underscoring that, in assessing the balance of convenience, the Supreme Court of Canada has cautioned that courts should refrain from attempting to ascertain whether harm to the public interest that has been identified by a public authority would actually result from the granting of injunctive relief. The Court explained that such an approach "...would in effect require judicial inquiry into whether the government is governing well, since it implies the possibility that the government action does not have the effect of promoting the public interest and that the restraint of action would therefore not harm the public interest": *RJR*, above, at 346.

[40] Further, I do not consider the fact that the AGC has relied on third-party reports to be determinative on its own. In view of the timing of the motion, the nature of the risks at stake, and the type of evidence in issue, I accept that third-party evidence may be sufficiently reliable for this motion, particularly as national security assessments focus on risk, which is necessarily forward-looking. The evidence also includes information on which bodies control or have the ability to exert influence over the Applicants, which is relevant to determining whether Hikvision is a State-Owned Enterprise [SOE] (section 3 of the ICA); it is not as limited as the Applicants suggest.

[41] In his affidavit, Mr. McCarty refers to information provided in Hikvision Canada's ICA notification supporting that Hikvision is an SOE that is controlled or influenced, directly or

indirectly, by the PRC government. He refers to Hikvision's 2024 Annual Report which lists the CETC as the actual controller of Hikvision and the CETC's subsidiary, China Electronics Technology HIK Group Ltd [CETHIK], as the controlling shareholder. Mr. McCarty refers to additional information provided during the national security review indicating that two out of the nine members of Hikvision's Board of Directors hold positions within the Chinese Communist Party [CCP] Committee of CETHIK Group. As members of the Board of Directors, these individuals hold voting rights in accordance with Chinese Company Law. He notes ISED's *Guidelines on the National Security Review of Investments* which state that the Government of Canada will subject all foreign investments by SOEs, or private investors assessed as being closely tied to or subject to direction from foreign governments, to enhanced scrutiny under the national security review provisions of the ICA.

[42] Mr. McCarty refers to concerns regarding the PRC government's ability to require PRC citizens anywhere in the world to assist and cooperate with China's intelligence services in support of national intelligence work, citing CSIS' 2023 Annual Public Report and a report from the Center for Naval Analyses. He provides a copy of the 2024 CSIS report that refers to the PRC as posing "the greatest counter-intelligence threat to Canada", targeting all levels of government and Canadian citizens to advance the PRC's national interests. CSIS assesses that the PRC and CCP will remain "an enduring threat to Canada" and will likely continue cyber activity in 2025. The concerns of CSIS were echoed in the Canadian Centre for Cybersecurity's 2025-2026 National Cyber Threat Assessment report that refers to the PRC cyber program as "surpass[ing] other hostile states in both the scope and resources dedicated to cyber threat

activity against Canada." The report refers to the cyber program as having "global cyber surveillance, espionage, and attack capabilities".

[43] The McCarty affidavit highlights a report by the Atlantic Council referring to the Applicants' participation as a "Tier One" partner in the China National Vulnerability Database of Information Security [CNNVD]. The CNNVD is a cybersecurity vulnerability reporting program run by the Ministry of State Security [MSS], the PRC's civilian intelligence and security service. The report notes that China has previously "weaponized software vulnerabilities provided to its CNNVD".

[44] The affidavit also identifies a report from the Stimson Center, a United States-based research institution dedicated to educating government offices on international affairs, including on China's strategic intentions. This document reports on Hikvision's strong ties with Chinese government organizations, including the PRC's Ministry of Public Security. The Stimson Center raises concerns regarding Hikvision, including that Hikvision has won several surveillance contracts with the PRC's Ministry of Public Security, that Hikvision states in its investor prospectus that it receives strong financial support from the Chinese government, and that Hikvision has close ties with the CCP. The Stimson Center report states that in 2019, the *National Defense Authorization Act* in the United States officially banned the use of video surveillance and telecommunications equipment supplied by Hikvision to government agencies based on national security concerns. The McCarty affidavit refers to continuing concerns that resulted in the US Federal Communication Commission [FCC] prohibiting authorization of Hikvision equipment for import and sale in the United States in 2022.

[45] The actions taken by the United States regarding Hikvision as reported by the Stimson Center demonstrate that Canada is not alone in its national security concerns. The United States government employed similar measures to ban the use of Hikvision video surveillance and telecommunications equipment in all government agencies in 2019 as the Government of Canada implemented through its public statement banning the use of Hikvision equipment in government offices following the OIC, following with the even more restrictive ban in 2022.

[46] In *China Mobile,* Chief Justice Paul Crampton found reports like the ones discussed here to adequately substantiate the allegations that were made by that respondent of alleged espionage and foreign interference by the PRC with activities in Canada. Like *China Mobile,* in my view, the third-party reports discussed above provide sufficient reliable and objective support for the purposes of this motion of the public interest harms identified by the Respondent.

[47] Thus, I find there to be sufficient evidence to support the national security concerns identified in the OIC and that these concerns must be balanced in the Court's analysis.

(3) Balancing the harm

[48] The Applicants argue that the balance should lie in their favour because they have provided direct evidence of real and immediate irreparable harm if the OIC is not stayed. They note that the effect of the OIC relates solely to the proliferation of Hikvision Canada's products, which the OIC concludes will impact Hikvision Canada's market presence. In this case, the OIC will not remove Hikvision's products from the market as the products can still be purchased from third parties. The Applicants contend that the OIC will thus not serve to eliminate the national

security risks it seeks to protect. Rather, as products remain on the market, they will become less safe without the necessary support systems in place to address vulnerabilities, thereby adding to the possibility of greater harm overall.

[49] As highlighted by the Respondent, the ICA provisions on which the OIC is based, are by their nature necessarily forward-looking. They do not turn on what has happened in the past or in the present but refer to the Investment's future impact on Canada's national security and the evaluation of risk. As assessed here, the harm is tied to the expanded and sustained market penetration of the Applicants' products and the significant rate of increased sales per month ([redacted] of product through [redacted] dealers across Canada) which proliferates the associated risk of PRC espionage and other intelligence activities in Canada.

[50] In my view, the distinction made by the Applicants is not sufficient on its own to tip the balance in the Applicants' favour.

[51] The Applicants assert that the OIC will cause irreparable harm by permanently damaging Hikvision Canada's market share and destroying Hikvision Canada's business. As noted earlier, the Zhang affidavit speaks to the harm that Mr. Zhang states will be caused by Hikvision Canada ceasing its operations and winding up its business. Mr. Davis provides further evidence to explain the harm he asserts will be caused by severing Hikvision Canada's after sale support and vulnerability management. He states that this contradicts established guidance to provide timely patching and will make vulnerabilities more exploitable.

[52] The Applicants contend that this direct evidence details the various types of irreparable harm that will be suffered in a clear and concrete manner. This distinguishes the present case from *China Mobile* where no direct evidence of irreparable harm was provided. They argue that the harm here should therefore be afforded greater weight in the balance of convenience analysis. The Applicants refer to the comments made by Chief Justice Paul Crampton at paragraph 103 of his decision:

> [103] The Applicants have established that they will suffer some irreparable harm if the stay they seek is not granted and they ultimately prevail on the JR Application. This harm includes the permanent loss of some of CMI Canada's customers, employees and revenues. It also includes some reputational harm and the loss of CMI Canada's BITS Licence. However, in the absence of clear and non-speculative evidence to support the irreparable nature of those harms in a detailed and concrete way, it is very difficult to have a good sense of the extent to which those harms will actually be suffered if the stay is not granted. Accordingly, the weight those alleged harms merit in the overall balancing of convenience analysis is less than it would be if such evidence had been provided.
>
> [Emphasis added]

[53] I have carefully reviewed the evidence submitted by the Applicants. The evidence establishes that there will be commercial losses to Hikvision Canada, disruption to business relationships, continuing damage to reputation, and loss of employees if the stay is not granted. I accept that this harm includes a monthly sales revenue loss of [redacted], along with some irrecoverable lease expenses and other contractual fees that are dependent on Hikvision Canada's products. It also includes disruption of Hikvision Canada's relationship with its distributors along with the cancellation of orders, the removal of product supports (safety, warranty and service), and cybersecurity support and patching from Hikvision Canada until the application is determined. I also accept that by requiring Hikvision Canada to wind-up its business instead of

allowing it to divest its assets, an opportunity to mitigate losses through sale of assets is not possible. I have taken all of this into consideration in my analysis.

[54] However, there are some limitations in the Applicants evidence that make it difficult to ascertain the extent of harm that will occur:

- While the estimated loss of sales revenue is significant, it must be viewed in context and with an understanding of the company's overall finances, including whether removal of expenses may offset some of this loss. Evidence speaking to this context is not provided.

- The evidence is speculative as to whether Hikvision Canada's business relationships with its distributor network will be permanently lost or whether Hikvision Canada would be able to re-establish at least some of these relationships if the judicial review were successful. As noted by the Respondent, despite the public announcement after the OIC was made, Hikvision Canada's distributors reinstated cancelled orders and placed new product orders once the terms of the Extension Agreement took effect.

- There are insufficient details relating to the downstream obligations of the Applicants' distributors and their associated dealers and how they may be tied to the Applicants' products. Without these details, there is insufficient evidence to substantiate the claim that "as a consequence of the OIC, dealers will be exposed to contractual penalties of [redacted] percent of project value to their customers, estimated to be over [redacted]".

- There is no information on what if any impact a temporary business shutdown would have on Hikvision Canada's existing customers who maintain product. While there would be a temporary loss of customer support for products, it is unclear whether the products could be supported in another way, including by third parties.

- There are incomplete details relating to Hikvision Canada's lease agreements to properly evaluate the termination clauses and the resulting financial obligations. Similarly, there are only two service contracts referenced but the contracts are not provided and there is limited information regarding other third-party contractual obligations that would be dependent on the operation of Hikvision Canada.

[55] The OIC requires, as part of the wind-up of Hikvision Canada's business, that it terminate the employment of all individuals in Canada who are employed in connection with its operations, or who are operating under a contract for service. While I accept that this will result in the permanent loss of some employees, I am unable to conclude concretely from the evidence filed what further options may be available to employees in terms of alternate employment or rehiring if the application is granted. Further, the Applicants have not indicated how the termination of employment will roll out in view of the 120-day provision period.

[56] As highlighted by the Respondent, an express term of the OIC is that:

> 7(1) The Minister may at their own discretion or on the written request of Hikvision, extend any time limit set out in this Order if they are of the opinion that Hikvision is unable to meet its obligations within the time limit.

> (2) In determining the duration of an extension, the Minister must consider any plan provided under section 6 as well as the purpose of the Order.

[57] Thus, if consistent with the purpose of the OIC, it may be possible to develop a plan that mitigates certain aspects of this harm, and others, on agreement.

[58] While I agree that the evidence filed here is more fulsome than what was before the Court in *China Mobile* and as such that the allegation of harm by the Applicants should be afforded greater weight, I nonetheless find that there are still some limitations to the evidence that factor in the balancing exercise.

[59] The Applicants assert that the Extension Agreement runs contrary to the Respondent's arguments as it in effect grants an interim stay of the OIC. As the Respondent agreed to allow Hikvision Canada to restart its business and to continue its operations until the determination of this motion, the Applicants argue that the national security risks identified cannot be as serious as the Respondent alleges. The Applicants assert that this provides strong support for the interlocutory stay requested on the motion, which would simply extend the existing agreement for a further limited time.

[60] The Extension Agreement seems to be different here from that imposed in *China Mobile*. It causes me some pause, considering that the parties agreed to a schedule for this motion that took somewhat longer than what I might have expected for this type of urgent motion. However, I was also surprised that the Applicants did not take any steps when the application was brought to expedite the application as a whole. Requesting case management and seeking and accelerated

timetable of at least its own steps would have demonstrated an intention to try to minimize harm. The surrounding circumstances to explain some of these choices is lacking. Moreover, without a copy of the Extension Agreement and details relating to how the terms and schedule were determined, I am unable to conclude that the Respondent's agreement alone negates their position on this motion. This is particularly so as the time it will take to proceed to a judicial review (at least four months to complete steps as submitted by both counsel) and obtain judgment (likely several additional months thereafter) will be far greater than the time relating to this motion.

[61] It should also be noted that although the Extension Agreement is in place, Hikvision Canada continues to operate with litigation risk as it is fully aware of the OIC and that the requested stay may not be granted. The communications with distributors must be considered with this backdrop in mind. There is no evidence that the Respondent sought to exacerbate the harms by agreeing to the Extension Agreement.

[62] Weighing the evidence of the parties and all these factors, I am of the view that the serious public interest harms associated with the national security risks identified by the Respondent outweigh the commercial interest harms the Applicants have established they will suffer if a stay is granted. Further, even if I did consider the harms to be balanced, I would nonetheless conclude that on equitable grounds the stay should not be granted as the Applicants come to the Court with unclean hands.

[63] While Hikvision Canada commenced its operations in Canada in 2015 and was required to provide notification of its operations before they commenced or within 30 days thereafter, Hikvision did not do so until nine years later, in November 2024, and only after it was prompted by ISED. The fact that the Applicants may not have been aware of the requirements of the ICA or may have misunderstood those requirements is no excuse, particularly considering they are a sophisticated entity represented by counsel, with operations globally: see *China Mobile* at para 107. The harm now caused by Hikvision Canada being required to cease its operations and wind-up its business after these nine years, is harm that could have been avoided had a notification been filed in 2015 when the notification should have been filed. The harms that Hikvision Canada now claims will arise are a result of its own delay.

[64] While I agree with the Applicants that the Court is not bound to refuse the requested stay because of these circumstances (*The Minister of Citizenship and Immigration v Thanabalasingham*, 2006 FCA 14 at paras 9-10; *Hrvoic v Hrvoic*, 2023 ONCA 508 at para 18), it is a further equitable consideration in the Respondent's favour that mitigates against granting the requested stay and preserving the *status quo* (*China Mobile* at paras 52 and 107).

[65] For all these reasons, I find that the motion must be dismissed.

[66] Nonetheless, to try to minimize harm as much as possible, I will order that the proceeding continue as a specially managed proceeding and that a case management judge be appointed to assist the parties with setting a timely schedule for next steps and a hearing date for the application.

[67] As there was no request for costs made by the parties, none shall be awarded.

ORDER IN T-2284-25

THIS COURT ORDERS that:

1. This motion is dismissed**.**

2. This application shall continue as a specially managed proceeding and shall be referred to the Office of the Chief Justice for the appointment of a case management judge.

3. Within seven (7) days of the appointment of a case management judge, the parties shall provide a joint timetable for next steps, including dates of availability for hearing the application, along with mutual dates of availability for a case management conference.

4. There shall be no order as to costs.

"Angela Furlanetto"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-2284-25
STYLE OF CAUSE:	HIKVISION CANADA INC. AND HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD. v CANADA (ATTORNEY GENERAL)
PLACE OF HEARING:	TORONTO, ONTARIO
DATE OF HEARING:	SEPTEMBER 4, 2025
JUDGMENT AND REASONS	FURLANETTO, J
CONFIDENTIAL ORDER AND REASONS ISSUED:	SEPTEMBER 16, 2025
PUBLIC ORDER AND REASONS ISSUED:	SEPTEMBER 22, 2025

APPEARANCES:

Tudor Carsten Bentley Gaikis Yuxi (Wendy) Sun	FOR THE APPLICANTS
Roger Flaim Ani Mamikon Addison Leigh	FOR THE RESPONDENT

SOLICITORS OF RECORD:

DLA Piper (Canada) LLP Barristers and Solicitors Toronto, Ontario	FOR THE APPLICANTS
Attorney General of Canada Toronto, Ontario	FOR THE RESPONDENT