Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

CMD 21-H4.47

File / dossier : 6.01.07
Date: 2021-05-03
Edocs: 6555615

Oral Presentation

Written submission from Louis Bertrand

Exposé oral

Mémoire de Louis Bertrand

In the Matter of the

Darlington New Nuclear Project

Application to renew the nuclear power reactor site preparation licence for the Darlington New Nuclear Project

Commission Public Hearing

June 10, 2021

À l'égard de

Projet de nouvelle centrale nucléaire de Darlington

Demande de renouvellement du permis de préparation de l'emplacement d'une centrale nucléaire pour le projet de nouvelle centrale nucléaire de Darlington

Audience publique de la Commission

10 juin 2021

Canada

Requests of the Commission

Granting the requested 10-year licence extension is not in the public interest and the application should be turned down for the following reasons:

A. The licence application relies on the environmental assessment done as part of the original project review by the CNSC-CEAA joint review panel, but the conditions have changed substantially, enough to force a re-evaluation of the risks.
Specifically:

1. The cybersecurity threat landscape is significantly different than it was in 2009 and the risks and consequences have escalated.
2. Software and embedded microcontrollers are still prone to programming errors, transient single bit errors, and incorrect operation;

B. The existing licence is for site preparation yet the 10 year licence renewal application encompasses licensing and building a new nuclear power plant. No reactor technology has been selected but from OPG's announcements, the choices are narrowed down to a short list of so-called small modular nuclear reactors (SMRs), a substantially different set of technologies.

If not outright rejecting the application, the Commission should make it a condition of licensing that another full and public hearing be held following OPG's selection of reactor design to give the public an opportunity to examine the proposed project and evaluate the potential for accidents and exposure to releases of radioactive materials.

A.1: Cybersecurity

The past two years have been significant in the area of cybersecurity as new threat actors have emerged with connections to nation states and motives other than what we expect from "hackers". These advanced persistent threats may have cartoonish names like Cozy Bear, Deep Panda and Helix Kitten[1] but their methods and intentions must be taken very seriously. Being connected or even sponsored by nation states, these groups are skilled and well resourced. Their motives often align with nation state strategic goals: espionage and eroding confidence in public institutions with well planned high profile attacks[2]. The attacks are not acts of war, but neither are they benign. The buzzword "cyber warfare" may be considered a new form of Cold War.

SolarWinds

On December 8 2020, in a filing to the US SEC and a blog post on its web site, cybersecurity firm FireEye disclosed that some of the attacking software tools used by the firm to test client security had been stolen in a highly sophisticated attack[3]. At the time of writing, FireEye were collaborating with the FBI and DHS as well as Microsoft's security team to understand the methods used. In the blog post, FireEye CEO Kevin Mandia reported that this attack represented an unprecedented level of sophistication and operational security, pointing to a well funded group with access to the resources of a nation state[4].

While investigating their own attack, FireEye discovered that the initial breach was done with a compromised component of the Orion network monitoring and management suite supplied by security software vendor SolarWinds[5]. The compromised component dubbed SUNBURST was digitally signed by SolarWinds and downloaded over 12,000 times by SolarWinds customers in the public and private sectors prior to the discovery.

The attackers were able to not only penetrate victim networks, but establish a persistent presence for months, move throughout the network and compromise other systems. As evidenced by the theft from FireEye, they were able exfiltrate information. The other notable characteristic of this attack was the patience and effort to remain undetected, in contrast to the popular notion of hacking a site for pure vandalism or to steal data for the purpose of extortion. Although there are APTs known to be motivated by financial gain, this was not the case for the SolarWinds attack.

---

[1] Swiss Cyber Forum, “Advanced Persistent Threat (APT) Examples: The A-Z Guide,” Academic, Swiss Cyber Forum, October 28, 2020, https://www.swisscyberforum.com/guide-of-advanced-persistent-threat-apt/.

[2] Major Juliet Skingsley, “The SolarWinds Hack: A Valuable Lesson for Cybersecurity,” Think tank, Chatham House, February 2, 2021, https://www.chathamhouse.org/2021/02/solarwinds-hack-valuable-lesson-cybersecurity.

[3] Alfred Ng, “FireEye Hack: Cybersecurity Firm Says Nation-State Stole Attacking Tools,” *CNET*, December 8, 2020, https://www.cnet.com/news/fireeye-hack-cybersecurity-firm-says-nation-state-stole-attacking-tools/.

[4] Kevin Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” Commercial, *FireEye Blog* (blog), December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html.

[5] SolarWinds Worldwide, LLC., “SolarWinds Orion Platform,” Commercial, SolarWinds, accessed April 30, 2021, https://www.solarwinds.com/orion-platform.

STUXNET

The STUXNET malware was a worm, a piece of malware that, once downloaded by an unwitting user, is able to propagate from one computer to another without human intervention. This particular worm was discovered in June 2010 by Kaspersky labs and is blamed for the destruction of a number of uranium enrichment centrifuges at the Natanz facility in Iran (Iran has not confirmed those reports)[6].

The attack was seen as a "game changer" in the antivirus community. The program demonstrated unusually sophisticated techniques, able to propagate over a network as well as by sharing an infected USB thumb drive, then gaining administrator privilege and hiding itself from antivirus software. Once installed, the worm sought out Siemens Step7 software used to program PLCs and was able to tamper with the controllers. The initial program download file was properly signed with a digital signature to make it appear that it had come from a reliable company. Finally, the creators of the worm had detailed knowledge of industrial control systems and Siemens PLCs. As with SolarWinds, the size and sophistication of the worm points to a nation state with funding and development talent.

The response of the antivirus community to this "game changer" should be noted here in the context of cybersecurity and incident response in the nuclear industry. Antivirus researchers working for companies in a very competitive market were eager to share their reverse engineering findings by email and on private online forums, a cooperation that was unique to the antivirus community, and is now widespread among security researchers, as noted above for the SolarWinds attack.

The Aurora experiment

In a demonstration at the US Idaho National Laboratory in March 2007, a remote cyber attack compromised a digital protective relay on a diesel generator set and caused it to operate with reverse logic, thus provoking a catastrophic out-of-sync condition. When the generator was in sync with the grid, the protective relay opened, relieving the generator of its load. Running at no-load, the generator soon went out of sync and the hacked protective relay reconnected the generator, putting a destructively heavy load on the generator and its diesel engine. After a few disconnect-reconnect cycles in the space of two minutes, the generator set was completely destroyed.

An internal DHS slide presentation obtained through FOI access[7] points out that a malicious out-of-sync condition can also affect electric equipment in industries other than power generation.

[6] David Kushner, “The Real Story of Stuxnet,” *IEEE Spectrum* 50, no. 3 (March 2013): 48–53, https://doi.org/10.1109/MSPEC.2013.6471059.

[7] muckrock.com, “Aurora FOI Request, Department of Homeland Security FOIA 2014-HQFO-00514” (muckrock.com, August 3, 2014), 19, https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/#1212530-14f00304-documents.

The alarmist view is that it only took 30 lines of code to destroy the equipment, but the comforting view at the time was that the knowledge required to craft those lines is the domain of deeply knowledgeable experts. The truth is somewhere in the middle[8]. However, as demonstrated by the SolarWinds and STUXNET attacks, APT groups connected to national governments have the resources, extensive knowledge and patience to mount this kind of sophisticated attack.

December 2015 Ukraine blackout

The December 23, 2015 blackout of 225,000 customers of several power utilities in the Ukraine also tells the tale of a well planned and coordinated attack, likely by a group aligned with a nation state.

The attack disabled SCADA systems and disconnected substations while a flood of bogus phone calls blocked calls from affected customers and another piece of malware wiped the control computers clean to erase evidence[9] [10]. There is also the possibility that some of the attack was direct intervention by the adversary. As part of the attack, SCADA computers at substations were wiped so that work crews had to be dispatched on-site to manually reconnect circuit breakers. Finally, uninterruptible power supplies were disabled to further hinder recovery efforts.

Forensic analysis of the attack showed that the initial breach happened at least six months before the attack and that the attackers were able to move around in the network, pointing to a patient and skilful adversary. The initial breach was delivered by a phishing email carrying a malware attachment. One of the lessons from the Ukraine incident is that it could have been prevented with better employee security awareness and network monitoring[11].

Ukraine's president at the time, Petro Poroshenko, blamed Russia for multiple cyber attacks before and after the December 2015 blackout, stating that Russia was waging a "cyber war" against Ukraine[12].

NSO Group Trident attack against a human rights activist

In August 2016, Ahmed Mansoor, an internationally recognized human rights defender based in the United Arab Emirates (UAE) received messages on his iPhone offering "new secrets" about

[8] Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," *Strategic Insights* 10, no. 1 (Spring 2011): 15.

[9] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *WIRED*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[10] Cybersecurity & Infrastructure Security Agency, "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure," Governmental, Cybersecurity & Infrastructure Security Agency, August 23, 2018, https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

[11] Kelly Jackson Higgins, "Lessons From The Ukraine Electric Grid Hack," Commercial, DarkReading.com, March 18, 2016, https://www.darkreading.com/vulnerabilities---threats/lessons-from-the-ukraine-electric-grid-hack/d/d-id/1324743.

[12] BBC News, "Ukraine Power Cut 'Was Cyber-Attack,'" *BBC News*, January 11, 2017, https://www.bbc.com/news/technology-38573074.

detainees in UAE jails if he clicked on a link in the message. Having previously been the target of hacking attempts, he forwarded the messages to Citizen Lab at the University of Toronto. In partnership with security firm Lookout, Citizen Lab reverse engineered the attack[13] [14]. The link was found to be part of the infrastructure of NSO Group, an Israeli firm owned by a US equity firm that sells a product called Pegasus to governments for "lawful intercept". Had Mansoor clicked on that link, his iPhone would have downloaded the Trident exploit that is the attack vector in Pegasus, and the rest of the payload would have installed itself with "root" privilege and enabled the attackers to view his files, emails, messages as well as turn on the camera and microphone at any time.

Relevance to the present application

The relevance of these stories to the present application is to demonstrate that the threat landscape has indeed evolved since the 2009 EIS and that previous estimates of risks due to malevolent actions are likely inadequate. The overall conclusion is that the level of sophistication of actors linked to nation states, either directly or at arms length, makes it impossible to dismiss the threats, and that APTs are only going to get better and bolder.

The Aurora experiment proved that an attacker with deep knowledge of instrumentation and control systems could cause physical damage, while the STUXNET and Ukraine attacks demonstrated that the threat is no longer theoretical. To dismiss the likelihood of a damaging attack by assuming that the "hackers" would not know the details of instrumentation and control systems is known as security-through-obscurity and is at best a dangerous delusion. The only safe stance is to assume that the "black hats" know more than the "white hats".

The SolarWinds attack, and to a certain extent the STUXNET worm, demonstrate that the supply chain is vulnerable to attack and that the distribution of compromised software by an unsuspecting vendor acts as a threat multiplier. The fact that the compromised package was part of the Orion network monitoring platform makes the supplier chain vulnerability that much more dangerous.

The relevance of Ahmed Mansoor's story is that sophisticated attack tools are available for sale by legal albeit shady suppliers like NSO, or on the black market. Smaller nation states pursuing their own strategic goals but lacking the necessary talent and infrastructure can nonetheless present a threat because they are able to hire the talent and malware.

[13] Bill Marczak and John Scott-Railton, “The Million Dollar Dissident: NSO Group’s IPhone Zero-Days Used against a UAE Human Rights Defender,” Research, Citizen Lab Research Report (Toronto: Citizen Lab, U. of Toronto, August 24, 2016), https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.
[14] Lookout Inc. and Citizen Lab, “Technical Analysis of Pegasus Spyware: An Investigation Into Highly Sophisticated Espionage Software,” Research (San Francisco, August 25, 2016), https://blog.lookout.com/trident-pegasus.

Cultural and technical challenges

One of the themes of the Chatham House 2015 report on cybersecurity in nuclear power plants[15] is the cultural challenge in bridging the domains of nuclear plant operations and cybersecurity. Specialists from each domain may have trouble finding a common language or sharing priorities. Furthermore, there is a general reluctance in any operational domain -- not just the nuclear industry -- to understand the implications of cybersecurity. It is often viewed as an unnecessary impediment.

The previously discussed incidents show that threats and threat actors are constantly evolving and that a generic security stance is no longer appropriate. Of particular concern are the regulatory and guidance documents CSA standard N290.7-14 "Cyber security for nuclear power plants and small reactor facilities" and CNSC REGDOC-2.5.2 "Design of Reactor Facilities, Version 2". Strict compliance with these documents may no longer be enough to ensure security from the emerging threats posed by highly competent groups.

CSA standard N290.7-14 discusses cybersecurity at a high level but does not venture into specifics. This in itself is not of concern however the overall mindset seems to treat cybersecurity as a static environment with nondescript threats. The standard was originally published in 2014 and reaffirmed in 2021, apparently without modification. It would be reasonable to question its relevance in the light of recent trends.

CNSC REGDOC-2.5.2 has the same static outlook. In section 5.22.4 "Cyber security", the advice is prudent and reasonable but implies a static cybersecurity stance. Interestingly enough, REGDOC-2.5.2 lists many resources for further reading but N290.7 is not in the list.

There is a need to broaden the definition of a cybersecurity incident to encompass the discovery of a serious vulnerability and the requirement to take immediate mitigation measures, either patching the software or implementing a work-around. Neither document addresses the need for rapid response to a vulnerability announcement. Operational issues are reviewed for cybersecurity implications, as they should be, but not the other way around. For example, N290.7 section 4.4.9 "Interface with operations and maintenance":

> *The cybersecurity program shall interface with the operations and maintenance programs to ensure that the operating procedures, maintenance procedures, work plans and work order instructions applicable to CEAs [cyber essential assets] implement and sustain cyber security controls.*

This is where I see a conflict between the nuclear plant operations in which modifications are carefully planned, reviewed and implemented, and cybersecurity where zero day exploits require immediate attention and mitigation. For example, if a controller was suspected to have been updated with malicious firmware, yet waiting for a command to activate the attack, could

[15] Caroline Baylon, Roger Brunt, and David Livingstone, “Cyber Security at Civil Nuclear Facilities: Understanding the Risks (Executive Summary)” (London: Chatham House, the Royal Institute of International Affairs, October 5, 2015), https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks.

operations continue while the component is taken out of service to replace the controller? If the controller is a primary safety essential device, the decision for example, to shut down a reactor would be reasonably justified, but in the case of a secondary device, the decision is not as clearcut. If a particular model of controller is in use throughout the NPP, would the entire plant be impacted? Or if the discovery of the compromise occurred during a season of peak electricity demand? Would security win over operations?

RECOMMENDATION 1: CSA N290.7 and CNSC REGDOC-2.5.2 should be updated to expand the incident response umbrella to chart a procedure to update CEAs in response to newly discovered threats. Just as the application of security measures is examined at the design stages, the procedure to upgrade firmware or apply mitigation measures should be part of the planning.

RECOMMENDATION 2: CSA N290.7 sections 8.4 and 8.5 should be expanded to encompass contingency planning for vulnerability notification, evaluation and response. When a vulnerability is discovered, either in-house, disclosed privately by the vendor, or widely published in the information security community, the response should be part of the contingency and continuity planning for the given CEA.

The Chatham House report also notes that the nuclear industry lags behind other industries in their approach to disclosure incidents and information sharing. Recall that in the SolarWinds case, vendors, security researchers and government agencies were collaborating openly. For the STUXNET worm, competitors in the antivirus market shared information freely about the methods employed by the malware and signatures to detect its presence.

CSA N290.7 section 4.4.6 "Interface with incident response" seems inadequate to ensure the necessary free and open discussion. The section suggests that not all incidents are reportable and does not set an upper bound on what is not reportable. The warning note that sharing operating experience (OPEX) should not disclose information that could lead to compromise of a CEA is of course prudent but the reporting requirements are left too vague.

RECOMMENDATION 3: Licensees should be mandated to report cybersecurity incidents to the appropriate security agencies (for example, CSE Canadian Centre for Cyber Security) as well as the usual reporting to the CNSC. This would remove one degree of separation between the victim organization and the agencies most directly involved in cybersecurity at the national level.

A more recent report from Chatham House[16] suggests that there is an opportunity for security-by-design in new builds though the time between design freeze and construction means that the designs will not keep up with rapidly evolving technology.

[16] Roger Brunt and Beyza Unal, “Cybersecurity by Design in Civil Nuclear Power Plants,” Briefing (London, UK: Chatham House, the Royal Institute of International Affairs, July 24, 2019), https://www.chathamhouse.org/2019/07/cybersecurity-design-civil-nuclear-power-plants.

A.2: Increased reliance on software for instrumentation and control systems (ICS)

In my intervention before the CNSC-CEAA joint review panel on the Darlington New Build [PMD11P1.182 April 1 2011], I discussed several concerns about the increased reliance on embedded microcontrollers and the software running on them that define their functioning.

Those concerns were and still are:

- The increased likelihood of single bit "soft" errors, either transient in a combinational network, or latched into a memory element (RAM cell or flip-flop) causing a single event upset (SEU). Since then, IC fabrication geometries have shrunk and logic supply voltages have dropped even more. It is now common for logic ICs, for example, RAM based field programmable gate arrays (FPGA), to operate on 1.2V or less. These two trends combine to increase the probability of a bit error. In software, that bit error may have no effect, or it may have a catastrophic consequence -- there is no way of predicting the impact.
- The difficulty of producing error free software. Software engineering procedures and processes have greatly increased software reliability, provided that they are applied in development. There are many surveys that point out that those procedures are often not applied, or applied inconsistently due to deadline pressure.

<u>Software errors: Boeing 737 MAX</u>
In the discussion about the quality of embedded control software, it is useful to consider the case of the Boeing 737 MAX that was grounded worldwide after two fatal crashes attributed to faulty software.
The more fuel efficient MAX had larger engines that its predecessor and to keep the same ground clearance, they were mounted higher and more forward. In normal flight, the engine pods do not generate lift but at a high angle of attack, they contribute to the lift. Being forward of the centre of gravity, the lift from the engine pods tend to increase the angle of attack in a positive feedback loop. To prevent a stall, Boeing engineers applied a software solution called the Maneuvering Characteristics Augmentation System (MCAS). Under certain conditions, it corrected the stabilizer trim to force the aircraft to pitch down if the system perceived a too high angle of attack in order to prevent a high speed stall. In the crashes, the software only considered one of the two angle-of-attack (AOA) indicators because the feature that added a warning to the instrument panel if the two AOAs disagreed was an option that the two airlines involved in the crash had not ordered (it is now in the base model).

The fault was attributed to the MCAS responding to the faulty AOA indicator that recorded an incorrect higher angle of attack than the actual figure, and MCAS forced the aircraft to pitch down, overruling the pilot. The pilots involved had not been trained in the operation of MCAS and were not aware of the override procedure.

The better way to study the 737 MAX is to consider that the software and the unreliable angle-of-attack (AOA) indicator were only the proximate cause of the accidents, but that the root cause was a system failure due to Boeing management pressure to keep up with competition

from Airbus, FAA regulators delegating inspection duties to Boeing, and airlines demanding ever more fuel efficient aircraft that minimize additional pilot training.

Ultimately, the failure can be attributed to conflicting goals: an accelerated development schedule compromising safety. It is unlikely that anyone at Boeing or the FAA framed it in such stark language, but this was the end result.

Bringing this back to the development of new technology nuclear reactors, the same concern over conflicting goals of accelerated development to meet self imposed deadlines (in operation by 2028) against a more cautious approach may have serious repercussions.

RECOMMENDATION 4: The Licence Condition Handbook should specify that the development of operating software for any new build must be audited to question assumptions that software can be made to compensate for undesirable reactor or plant operating characteristics.

B. Building an Experimental Reactor Is Not Simply "Site Preparation"

The environmental impact assessment dates back to 2009 and was submitted to the CNSC-CEAA joint review panel (JRP) in 2011. In the original application, the Plant Parameter Envelope (PPE) included up to 4800MWe of conventional CANDU or light water reactors, and there are many such installations in Canada (CANDU) and around the world (LWR/PWR), and there is sufficient operational experience to evaluate the risks and benefits.
However OPG's proposed new build is for one of three designs of small modular nuclear reactors (SMRs), contradicting OPG's statements in section 4.3 of the application that "no revisions are required to the PPE as no significant gaps have been identified that would alter the existing PPE".

These new reactors are claimed to offer inherent safety advantages and economies of scale yet are unproven except for demonstration scale prototypes. Building a grid scale reactor at Darlington cannot be considered as anything other than an experiment and as such requires a thorough public review of the licence application.

The proposed reactors, GE Hitachi BWRX-300, Terrestrial Energy Integral Molten Salt Reactor (IMSR) and the X-Energy XE-100, use enriched uranium prepared in unconventional containment. The high level waste will have a different composition and activity level than the waste currently stored on-site at Darlington. The chemical composition of the wastes is also unknown, given that they may be treated chemically before storage.

Two of the proposed SMRs, GE Hitachi BWRX-300 and Terrestrial Energy’s IMSR, are meant to be built below grade. Although burying the reactors appears to improve shielding, it also prevents the containment to be inspected from the outside. Furthermore, it would invalidate parts of the environmental assessment since the original plan was for a ground level build. At the very least, the geology must be reconsidered to understand the potential for ground shifting and effects on ground water.

RECOMMENDATION 5: The environmental assessment must take into account the geology of the site and its ability to accept a below grade build and resist shifting due to ground water, shoreline erosion or earthquakes.

The Terrestrial Energy’s IMSR molten salt and X-Energy's gas cooled SMR proposals operate at extremely high temperatures and pressures. As the saying goes, in theory, theory and practice are the same; in practice, they're not. The pressure and temperatures involved place extreme requirements on the containment and operating equipment and the reliability of the system can only be determined when it is in full operation. It's a bit of a Catch-22 -- the design cannot be proven without testing, but testing cannot begin until the design is proven.

The proposed new designs are also a departure from the Canadian experience in that they are designed and built by private corporations, whereas previous CANDU plants were designed and built by public sector organizations: AECL and provincial electric utilities (Ontario Hydro and its

successor OPG). Being public or semi-public institutions, the designs were accessible for review by regulators and interested parties. However the potential SMR vendors competing with each other have an interest in keeping as much of their designs proprietary and this could hinder a comprehensive safety and performance design review or incident response and investigation.

Upstream and downstream effects out of scope

Current practice in environmental assessment require the examination of several factors not considered in the 2009 EIS, specifically upstream and downstream impacts. The upstream mining of uranium ore disproportionally impacts the traditional territories of indigenous First Nations[17] [18] and must be considered in the overall project. The downstream multi-generational storage of high level radioactive waste on site impacts future generations though they will not benefit from current electricity production. In both cases, one can argue that the project is generally "in the public interest" while remaining blind to some very real ethical and moral considerations of fairness and equity. The difficulty of attributing a specific illness to radiologic pollution offers a convenient loophole to disavow responsibility.

At this point, there has been little, if any, public discussion through the CNSC licensing process of the expected inventory of new radioactive wastes and what to do with them at the end of the useful life of the reactors, some 60 or more years from now. Although most of us participating in this licensing process will be either retired or gone, those wastes will still be lethal.

RECOMMENDATION 6: The Commission should require in the LCH that the licensee detail plans for the long term storage of high level radioactive and/or wastes on the Darlington site before any permit to proceed with construction is issued.

RECOMMENDATION 7: The Commission should require in the LCH that the licensee must detail the quantities and composition of high level radioactive and/or toxic wastes expected to be produced by the new reactor when the technology is selected and before any permit to proceed with construction is issued.

[17] Geoffrey Bird, “Legacy of Canada’s Role in Atomic Bomb Is Felt by Northern Indigenous Community,” *Canadian Geographic*, August 21, 2020, https://www.canadiangeographic.ca/article/legacy-canadas-role-atomic-bomb-felt-northern-indigenous-community.

[18] Atanu Sarkar et al., “Environmental Impact Assessment of Uranium Exploration and Development on Indigenous Land in Labrador (Canada): A Community-Driven Initiative,” *Environmental Geochemistry and Health* 41, no. 2 (April 1, 2019): 939–49, https://doi.org/10.1007/s10653-018-0191-z.

Summary of Recommendations

1: CSA N290.7 and CNSC REGDOC-2.5.2 should be updated to expand the incident response umbrella to chart a procedure to update CEAs in response to newly discovered threats. Just as the application of security measures is examined at the design stages, the procedure to upgrade firmware or apply mitigation measures should be part of the planning.

2: CSA N290.7 sections 8.4 and 8.5 should be expanded to encompass contingency planning for vulnerability notification, evaluation and response. When a vulnerability is discovered, either in-house, disclosed privately by the vendor, or widely published in the information security community, the response should be part of the contingency and continuity planning for the given CEA.

3: Licensees should be mandated to report cybersecurity incidents to the appropriate security agencies (for example, CSE Canadian Centre for Cyber Security) as well as the usual reporting to the CNSC. This would remove one degree of separation between the victim organization and the agencies most directly involved in cybersecurity at the national level.

4: The Licence Condition Handbook should specify that the development of operating software for any new build must be audited to question assumptions that software can be made to compensate for undesirable reactor or plant operating characteristics.

5: The environmental assessment must take into account the geology of the site and its ability to accept a below grade build and resist shifting due to ground water, shoreline erosion or earthquakes.

6: The Commission should require in the LCH that the licensee detail plans for the long term storage of high level radioactive and/or wastes on the Darlington site before any permit to proceed with construction is issued.

7: The Commission should require in the LCH that the licensee must detail the quantities and composition of high level radioactive and/or toxic wastes expected to be produced by the new reactor when the technology is selected and before any permit to proceed with construction is issued.