December 15, 2015

Honorable Harjit S. Sajjan
Minister of National Defense
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Mr. Sajjan,

Threat to Canada's National Security

Please ensure that Defense Minister Sajjan sees this, so that he can judge for himself the veracity and strategic importance of what it is I wish to bring to his attention – which is diametrically opposed to what Industry Canada, Health Canada, the Canadian Wireless and Telecommunications Association (CWTA), all wireless and telecom companies, and all electric power utilities across Canada tell governments and the public today (The same is true in all Western countries.) Let me explain.

I am a retired Canadian Armed Forces captain, who spent 22 or his 26+ years in Canada's military in the arcane fields of Electronic Warfare (EW) and Signals Intelligence (SIGINT). My most significant appointments included: two years in National Defense Headquarters in the Directorate of Electronic Warfare (DEW) in which I was the sole EW officer charged with supporting Canada's only army EW company. For two years I worked closely with U.S. and NATO army EW units and completed a lengthy NATO army EW officers' course in Anzio, Italy, and participated in a major NATO army EW officers' field exercise in Germany. I also accepted invitations to visit the U.S. Pentagon and, separately, Fort Bragg, N.C., the U.S. Army's major EW base. My previous two-year posting was in the SIGINT world, where I was appointed the Executive Officer and Operations Officer at one of Canada's largest and most sensitive SIGINT radio stations, where approximately 200 specially-trained radio intercept operators reported directly to me. Earlier in my career I had conducted Radio Warfare at sea aboard two Canadian warships.

Preposterous though it may sound, this letter provides Defense Minister Sajjan with an historic opportunity to truly distinguish himself – and Canada – from every other Western country in the world! Minister Sajjan should be interested to note that in 2012 I wrote, initially, to Peter McKay, Canada's then Minister of National Defense, then, to Canada's Prime Minister, Stephen Harper, warning both of them that Industry's use of wireless radio technology was posing the greatest single threat to Canada's National Security in our country's entire history! Both of my letters were completely ignored; nor did I even receive an acknowledgement from either office that my letter had been received! Yet in both letters I made it abundantly clear that Industry Canada's decision to allow the electric power industry to use "***wireless***" radio technology to operate, maintain and control Canada's electric power grid was absolutely indefensible and

completely inexcusable! I am absolutely confident that my harsh criticism of Industry Canada would readily be supported by Canada's CSE (Communications Security Establishment) and our top military communications experts, i.e., the Director General, Intelligence and Security (**DGIS**), the Head of the Directorate of Electronic Warfare (**DEW**) or the Head of the Communications Electronics Engineering (**CELE**) Branch.

You may be aware that I have previously exchanged correspondence on this subject with the Minister of Industry Canada, who lamentably delegated my letter to his Director National Telecommunications Security: Mr. Guy Mitchell, with whom I've since had an entirely unsatisfactory exchange of emails. Consequently, I have no recourse but to bring this matter to your personal attention – because it is a matter of grave concern for Canada's National Security! Exactly the same situation exists in the U.S.; although they appear to be trying to address the problem (see below).

http://frontpagemag.com/2012/jamie-glazov/an-electromagnetic-pulse-catastrophe/
"Dr. Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security who advises Congress on the full spectrum of security issues. He is now focused on preventing a nuclear or natural electromagnetic pulse (EMP) catastrophe– the greatest threat now facing civilization. Dr. Pry has spent his entire career protecting America from Weapons of Mass Destruction and EMP, first at the Central Intelligence Agency, then at the House Armed Services Committee, on the Congressional EMP Commission and Strategic Posture Commission. He is the author of the new book, Civil-Military Preparedness For An Electromagnetic Pulse Catastrophe, a Kindle e-book available on Amazon.com"

As a retired Signals Intelligence and Electronic Warfare Officer, with almost 27 years' experience, it is my personal opinion that either: Industry Canada does not have the requisite professional expertise in house to fully appreciate the vulnerabilities of ***wireless*** radio communications; or else someone in Industry Canada is in collusion with the telecom industry, headed up by Mr. Bernard Lord, QC, ONB, who is the President and CEO of the Canadian Wireless and Telecommunications Association. Regardless of why "***wireless***" radio was chosen, that decision should never have been made in the first place and needs to be rescinded – immediately! Some of the more obvious reasons why "***Wireless***" technology should never be used on any of Canada's critical infrastructure are:

- Electronic warfare experts in all militaries of the world know that ***wireless*** radio communications are the easiest technology to interfere with, disrupt or neutralize.

- Electronic warfare weapons stemming from the Cold War and even World War II. such as "Window" "Rope" "Chaff" and a host of single or multiple-frequency radio "jammers" can easily disrupt, defeat and totally block ***wireless*** radio communications rendering them useless;

- Severe electrical storms can play havoc with ***wireless*** radio systems, interrupting large regions of the country for the duration of the electrical storm;

- Naturally occurring Electromagnetic Pulses (EMPs), e.g., solar storms, solar flares (which can release large bursts of energy, including electrons and atoms from the sun's corona) can literally "fry" or incinerate any **"wireless"** radio system;

- EMP weapons can be classified as nuclear, high powered microwave (HPM) or electromagnetic bomb (or e-bomb). All are weapons with scalable foot prints, meaning they can all "kill" (incinerate) electronic systems in an area ranging in size from a tennis court to the entire continental United States! "An EMP attack is as instantaneous as an atomic bomb blast. It moves like a wall of energy overloading, and destroying all computer based technology. Such an attack would shut down any power grid. Air traffic would be grounded; telephone, internet and other communications would be shut down. America would be reduced to the agricultural economy we had in the 1800s." (Note: EMP weapons don't hurt people directly.)

- HPM weapons are non-nuclear, operate in the 1 MHz-1 GHz range, and can be tailored to generate area effects or to target an individual aircraft or vehicle. Current power densities vary between 0.1 w/m2 to 100 w/m2. Countries that have purchased or are developing HPM weapons include: the U.S, Russia, Australia and Sweden;

- High Altitude EMP (HEMP): "a detonated nuclear device high above the earth could cripple electronic systems, knock out water and electricity supplies and bring civilization to a halt. The abrupt pulse of EMR from a large explosion, such as that produced by a nuclear weapon high above the earth, produces rapid changes to electric and magnetic fields that generate surges in voltage and current inside electronic equipment - burning out microchips and circuitry. Currently, the U.S., Russia, China, India, the United Kingdom, France, Pakistan and Israel have the capability to produce HEMP, and 11 other countries are not far behind." (Note: Iran has recently tested its own EMP.)

- Both the U.S. and Russia have had electronic weapons of mass destruction for more than 20 years, in the form of "HAARP" (High Active Auroral Research Project). Essentially, these are High Frequency (HF) radio transmitters capable of emitting highly-focused, billions of watts up into the ionosphere such that the resultant "pulse" would be reflected or bounced back down to earth, at the speed of light, with such force and pin-point accuracy that it would destroy/incinerate its intended target.

- Cyber attacks employing sophisticated malware, such as Stuxnet, Flame and Duqu could easily wreak havoc on any ***"wireless"*** electric power grid system.

From the above it should be obvious that, had the Federal Government consulted with its own military communications experts – DGIS; DEW, CSE or the CELE Branch - prior to making its ill-conceived decision to choose the "***wireless"*** option, they would have been strongly advised not to do so. For such a critical application as Canada's electric power grid, military experts would caution Government to consider only robust technologies, such as buried fiber optic cable, that can be further "hardened" at critical locations, as and where needed. In this way, Government could be assured Canada's electric power grid had a meaningful degree of survivability, security, reliability and dependability, which would greatly enhance Canada's ability to withstand all but the most severe and determined attacks.

As Canada's Minister of National Defense, Mr. MacKay, I urge you to personally intervene – ***immediately,*** while there is still time - and exercise the powers of your office to rescind Industry Canada's utterly stupid and completely indefensible decision to select "***wireless***" radio technology to operate and control Canada's electric power grid. Unless that decision is overturned, all Canadians will be exposed to the greatest threat this country has ever faced! And that will be your legacy.

Respectfully yours,
James G. Flynn
Kelowna, B.C.