Melissa Hoffer
Assistant Attorney General
Via Email: melissa.hoffer@massmail.state.ma.us

April 4, 2016

Hello Melissa:

RE: Post Operations Spent Fuel Storage & Security

The British press reported that the plane that crashed in Pennsylvania on 9/11 was headed to Three Mile Island. One of the principal fears at Fukushima was that one of the spent fuel pools would fail. Concerns about nuclear terrorism rose again after Belgian media reported that suicide bombers who killed 32 people in Brussels on March 22 originally looked into attacking a nuclear installation and switched targets only because of police raids that netted a number of suspected associates.

It is critically important to significantly reduce the vulnerability of Pilgrim's spent fuel. We ask that you take the following actions to do so:

1. Support use of Pilgrim's decommissioning trust fund (DTF) to ensure that spent nuclear fuel is moved from the spent fuel into dry casks as quickly as possible. The NRC should condition any such use on (or you should obtain Entergy's agreement requiring) depositing any monies recovered by Entergy in its suits against DOE for breach of contract in the DTF to replenish the DTF.

2. Advocate use of a different dry cask storage system – either Holtec Hi-Storm 100-U modules or hardened dry casks surrounded by earthen berms – to enhance security, and to locate casks on higher ground to protect against rising sea levels.

Spent Fuel Pool

The most important thing is to take every available step to insure that Pilgrim's spent fuel is moved from the spent fuel into dry casks as quickly as possible.

Vulnerability: Reactors make ideal targets. Despite the fact that they contain large amounts of radioactivity that could create severe impacts, they are highly vulnerable and poorly defended, particularly against small aircraft. According to a report done by your office in 2006,[1] a spent fuel pool fire at Pilgrim could result in up to $488 billion dollars in damages, 24,000 latent cancers and contamination hundreds of miles downwind. Your office showed that the design of reactors like Pilgrim, GE BWR Mark

[1] The Massachusetts Attorney General's Request for a Hearing and Petition for Leave to Intervene With respect to Entergy Nuclear Operations Inc.'s Application for Renewal of the Pilgrim Nuclear Power Plants Operating License and Petition for Backfit Order Requiring New Design features to Protect Against Spent Fuel Pool Accidents, Docket No. 50-293, May 26, 2006 includes a Report to The Massachusetts Attorney General On The Vulnerability of Pilgrim's Spent Fuel Pool- Risks and Risk-Reducing Options Associated with Pool Storage of Spent Nuclear Fuel at the Pilgrim and Vermont Yankee Nuclear Power Plants, Gordon Thompson, May 25,2006

I's, make those reactors highly vulnerable to attack because their spent fuel pools are outside primary containment with a light roof structure overhead. Please see Attachment for more details.

Measures To Reduce Risk: Expedite transfer of the spent fuel from the pool to hardened dry storage. However, Entergy is unwilling to pay for transfer out of its current operating budget. The only reasonable option to protect public safety is to allow Entergy to use their decommissioning trust fund (DTF) for spent fuel management- amendments allowed by NRC for example at Vermont Yankee, Kewaunee, San Onofre.

We understand that the MAAGO has objected to using the DTF for this purpose at Vermont Yankee. We respectfully disagree. We know that the DTF will almost certainly not have enough money to pay all decommissioning costs, particularly if funds are withdrawn from it, but the potential cost to the Commonwealth of a spent fuel fire dwarfs any potential decommissioning shortfall.

We recommend that the MAAGO request that NRC require funds resulting from Entergy suing DOE for breach of contract for failing to take Pilgrim's fuel by 1998 be deposited in Pilgrim's decommissioning trust fund, at a minimum in the amount needed to replenish it for what was taken out, and preferably enough to cover future spent fuel management and other decommissioning costs.

If the NRC is not cooperative, you should seek, as did Vermont, to reach agreement with Entergy. You are probably aware that as part of the State of Vermont Settlement Agreement with EVY, ENO[2] agreed to deposit all reimbursement for SNF management expenses to be deposited "into either: (i) the NDT, or (ii) a separate trust …, provided that the funds in any such trust are: (1) dedicated to meeting the liabilities of EVY, including decommissioning, SNF management, and site restoration activities at the VY Station."

There is good reason to believe that Entergy would be receptive to such an agreement, since it has repeatedly told that NRC that it plans to move the spent fuel into casks within 5-6 years after shutdown. It seems particularly likely you would succeed in doing so as part of settling any dispute (e.g., the current NRC proceeding or if S. 1798 is passed by the Legislature) between Entergy and the Commonwealth.

The bottom line is that moving the fuel out of the pool as soon as possible is a win-win. It would be a win for public safety. It also would be a win for Entergy because its O&M costs (which it most certainly does not want to pay out of operating expenses) significantly decrease once spent fuel transfer out of the pool is completed.

Dry Cask Storage

Vulnerability: Pilgrim now has 3 dry casks; 5 more are planned this spring. Eventually there will be about 60 dry casks; and a few more if they refuel in the spring of 2017. Pilgrim's casks will be lined up vertically on a pad, in the open and vulnerable to attack – an arrangement referred to as "candlepin bowling for terrorists."

[2] file:///C:/Users/Mary/Documents/decomissioning/VERMONT/SETTLEMENT%20-site%20restoration/VY_Settlement_Agreement_131223.pdf

Pilgrim's defense is light in a military sense. Casks are vulnerable from an air or land-based attack, with weapons readily available today. [3] Pilgrim has no defense for an air attack. A Univ.Texas study team placed it among the seven most vulnerable reactors to a water based attack.[4] Frequent tresspassing events demonstrate its vulnerability from a land based attack. In addition, Pilgrim is located in "America's Hometown," making it a symbolic target. See Attachment for more detail.

Despite their vulnerability, the NRC commissioners voted on September 11, 2015[5] to postpone the schedule for developing new requirements for protecting spent fuel in dry cask storage from sabotage by five years. There are a number of good reasons to implement this rule sooner. The most important is that the current rules do not provide adequate protection of dry casks from certain types of terrorist attack scenarios, as even the NRC has acknowledged publicly.

MAAGO'a expert, Dr. Gordon Thompson, analyzed the impact of the shaped charge as a potential instrument of attack.[6] The analysis shows that the cylindrical wall of the canister is about 1/2 inch (1.3 cm) thick, and could be readily penetrated by available weapons.

---

[3] The Massachusetts Attorney General's Request for a Hearing and Petition for Leave to Intervene With respect to Entergy Nuclear Operations Inc.'s Application for Renewal of the Pilgrim Nuclear Power Plants Operating License and Petition for Backfit Order Requiring New Design features to Protect Against Spent Fuel Pool Accidents, Docket No. 50-293, May 26, 2006 includes a Report to The Massachusetts Attorney General On The Vulnerability of Pilgrim's Spent Fuel Pool- Risks and Risk-Reducing Options Associated with Pool Storage of Spent Nuclear Fuel at the Pilgrim and Vermont Yankee Nuclear Power Plants, Gordon Thompson, May 25, 2006;Environmental Impacts of Storing Spent Nuclear Fuel and High-Level Waste from Commercial Nuclear Reactors: A Critique of NRC's Waste Confidence Decision and Environmental Impact Determination, Dr. Gordon Thompson, February 6, 2009, pgs., 29, 47, 50, Tables 7-6, 7-7.

[4] http://sites.utexas.edu/nppp/files/2013/08/NPPP-working-paper-1-2013-Aug-15.pdf

[5] http://allthingsnuclear.org/elyman/ominous-votes-by-the-nrc

[6] Gordon R. Thompson, *Environmental Impacts of Storing Spent Nuclear Fuel and High- Level Waste from Commercial Nuclear Reactors: A Critique of NRC's Waste Confidence Decision and Environmental Impact Determination* (Cambridge, Massachusetts: Institute for Resource and Security Studies, 6 February 2009). Tables also in Declaration of 1 August 2013 by Gordon R. Thompson: Comments on the US Nuclear Regulatory commission's Draft Consequence Study of a Beyond-Design-Basis Earthquake Affecting the Spent Fuel Pool for a US Mark I Boiling Water Reactor

Table 7-7:Performance of US Army Shaped Charges, M3 and M2A3

Target Material	Indicator	Type of Shaped Charge	
		M3	M2A3
Reinforced concrete	Maximum wall thickness that can be perforated	60 in	36 in
	Depth of penetration in thick walls	60 in	30 in
	Diameter of hole	• 5 in at entrance • 2 in minimum	• 3.5 in at entrance • 2 in minimum
	Depth of hole with second charge placed over first hole	84 in	45 in
Armor plate	Perforation	At least 20 in	12 in
	Average diameter of hole	2.5 in	1.5 in

The spent fuel assemblies inside the canister are composed of long, narrow tubes made of zirconium alloy, inside which uranium oxide fuel pellets are stacked. The walls of the tubes (the fuel cladding) are about 0.023 inch (0.6 mm) thick. Zirconium is a flammable metal.

Consequences of a Cask Release: As shown in Dr. Thompson's table, casks are not robust in terms of their ability to withstand penetration by weapons available to sub-national groups. A typical cask would contain 1.3 MCi of cesium-137, about half the total amount of cesium-137 released during the Chernobyl reactor accident of 1986. Most of the offsite radiation exposure from the Chernobyl accident was due to cesium-137. Thus, a fire inside an ISFSI module, as described in the preceding paragraph, could cause significant radiological harm.

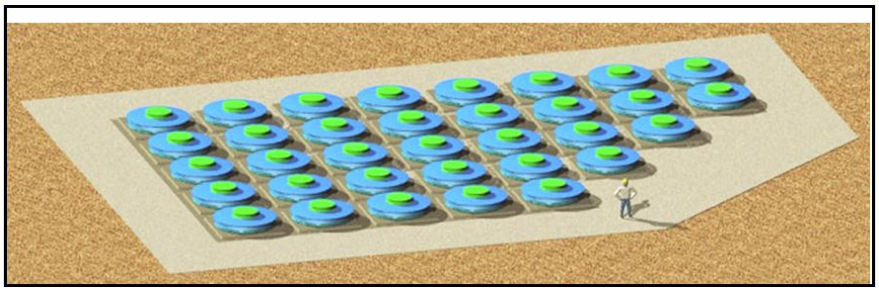
Measures to Reduce Risk:

1. Disperse the casks and mound with dirt berms. Pilgrim has plenty of acreage between Rocky Hill Road and Route 3A. This acreage that has the added advantage that it is far enough above sea level to remain above water as sea levels continue to raise over the decades that the fuel is likely to be onsite.

Solution: Safer Dispersed/Hardened Dry Cask Storage- Literally, Dirt Cheap

2. Use Holtec Hi-Storm-100U casks that employ the same canister used in the present Holtec modules, as is being done at San Onofre.

   For most of its height, the 100U module would be underground.



http://www.holtecinternational.com/productsandservices/wasteandfuelmanagement/hi-storm/hi-storm-100u/

Holtec described the robustness of the 100U module as follows[7]:

> "Release of radioactivity from the HI-STORM 100U by any mechanical means (crashing aircraft, missile, etc.) is virtually impossible. The only access path into the cavity for a missile is vertically downward, which is guarded by an arched, concrete-fortified steel lid weighing in excess of 10 tons. The lid design, at present configured to easily thwart a crashing aircraft, can be further buttressed to withstand more severe battlefield weapons, if required in the future for homeland security considerations. The lid is engineered to be conveniently replaceable by a later model, if the potency of threat is deemed to escalate to levels that are considered non-credible today."

Thank you in advance for your attention and we look forward to your response and would be happy to provide any additional information that might be helpful to you.

Mary E. Lampert
Pilgrim Watch
148 Washington Street
Duxbury, Massachusetts 02332
Email: mary.lampert@comcast.net
Tel: 781-934-0389

[7] Holtec International, "The HI-STORM 100 Storage System", accessed at <http://www.holtecinternational.com/hstorm100.html> on 17 June 2007.

ATTACHMENT
OVERVIEW SECURITY ISSUES

Pilgrim's (in)security - a symbolic target located in "America's Hometown"- no defense for an air attack; named among seven most vulnerable to water attack; frequent tresspassing events reported. Pilgrim is vulnerable to attack until all the waste leaves the site.

The terrorist threat did not end after 9/11; acts of malice can occur at random from other parties such as the likes of the Oklahoma Bomber. Dr. Edwin Lyman, Union of Concerns Scientists, warned in testimony submitted to the US Senate:

> "*If a team of well-trained terrorists were to succeed in gaining forced entry to a nuclear power plant, within a matter of minutes it could do enough damage to cause a meltdown of the core and a failure of the containment structure."*

Nuclear Reactors As Potential Targets Of Attack: Reactors make ideal targets because: they contain large amounts of radioactivity that could create severe impacts and their defense is "light" in a military sense. The design of GE BWR Mark I reactors like Pilgrim, make those reactors highly vulnerable to attack because their spent fuel pools are outside primary containment with a light roof structure overhead.

HOW SECURE ARE COMMERCIAL NUCIEAR REACTORS, SUCH AS PILGRIM?

Pilgrim is vulnerable to attack- while operating and when closed

The threat against nuclear power plants is real. According to the 9/11 Commission report, the Sept. 11, 2001 terrorists initially considered attacking a nuclear power reactor.[8] According to a **new report** "**Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current 'Design Basis Threat' Approach**,"[9] prepared under a contract for the Pentagon by the Nuclear Proliferation Prevention Project (NPPP) at the University of Texas at Austin's LBJ School of Public Affairs finds that none of the 104 commercial nuclear power reactors in the United States is protected against a maximum credible terrorist attack, such as the one perpetrated on September 11, 2001, nor against airplane attacks, nor even against readily available weapons such as rocket propelled grenades and 50-caliber sniper rifles.

The following table, prepared by Dr. Gordon Thompson for the Massachusetts Attorney General,[10] summarizes available means of attack. It shows that nuclear power plants are vulnerable.

---

[8] http://www.resilience.org/stories/2004-07-25/911-report-reveals-al-qaeda-ringleader-contemplated-ny-area-nuclear-power-plant-p

[9] http://sites.utexas.edu/nppp/files/2013/08/NPPP-working-paper-1-2013-Aug-15.pdf

[10] The Massachusetts Attorney General's Request for a Hearing and Petition for Leave to Intervene With respect to Entergy Nuclear Operations Inc.'s Application for Renewal of the Pilgrim Nuclear Power Plants Operating License and Petition for Backfit Order Requiring New Design features to Protect Against Spent Fuel Pool Accidents, Docket No. 50-293, May 26, 2006 includes a Report to The Massachusetts Attorney General On The Vulnerability of Pilgrim's Spent Fuel Pool- Risks and Risk-Reducing Options Associated with Pool Storage of Spent Nuclear Fuel at the Pilgrim and Vermont Yankee Nuclear Power Plants, Gordon Thompson, May 25, 2006

Mode Of Attack	CHARACTERISTICS	PRESENT DEFENSE
Commando-style by land	• Could involve heavy weapons/sophisticated tactics • Attack requiring substantial planning and resources	Alarms, fences, lightly-armed guards, with offsite backup
Commando-style by water	• Could involve heavy weapons/sophisticated tactics • Could target intake canal • Attack may be planned to coordinate with a land attack	500 yard no entry zone – marked by buoys – simply, "no trespassing" signs Periodic Coast Guard surveillance by boat or plane
Land-vehicle bomb	• Readily obtainable • Highly destructive if detonated at target	Vehicle barriers at entry points to Protected Area
Anti-tank missile	• Readily obtainable • Highly destructive at point of impact	None if missile is launched from offsite
Commercial aircraft	• More difficult to obtain than pre-9/11 • Can destroy larger, softer targets	None
Explosive-laden smaller aircraft	• Readily attainable • Can destroy smaller, harder targets	None

Aircraft: Although the NRC has required that <u>future</u> reactors be designed to mitigate attacks by commercial aircraft, it has not required existing reactors to make retrofits to address that threat, such as the "beamhenge" shield design.[11] That design, places tall beams around the reactor with cables strung between to break up the wings of in-coming planes.

An air attack is likely from a smaller, general-aviation aircraft laden with explosive material or simply a full load of fuel. The US General Accounting Office (GAO) expressed concern, in September 2003 testimony to Congress, about the potential for malicious use of general-aviation aircraft. The testimony stated:

> Since September 2001, TSA [the Transportation Security Administration] has taken limited action to improve general aviation security, leaving it far more open and potentially vulnerable than commercial aviation. General aviation is vulnerable because general aviation pilots are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports. Over 550 of these

[11] http://committeetobridgethegap.org/beamhenge/

airports also provide commercial service. In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists.[12]

Pilgrim's spent fuel pool is especially vulnerable. The roof over the pool is light- weight. It was designed to give in a reactor core accident so as to allow the radioactive plume to extend upwards into higher elevations. It is easily penetrable. Pilgrim's outer wall is approximately 2' reinforced concrete and the wall around the spent fuel pool is 5' thick. Attack by air or land with todays readily avaialble sophiticated weapons could penetrate the walls.

Drones: Drones pose a number of security concerns for nuclear reactors. The concern is not small payload drones delivering explosives because most of the vital equipment is already hardened against hand-carried explosives. Rather, the concern is largely that drones could enhance tactical advantage. For example, drones could distract the security guard force during a ground attack, slowing their response or causing them to be mispositioned to the advantage of the attackers; and drones could target the security cameras, motion sensors, etc. to mask ground attackers. The timelines for security force personnel to deploy and prevent attackers from successfully sabotaging key equipment are short. Anything that prevents timely and proper response by the guard force could be a problem.

Water-Based Attack: Pilgrim is on Cape Cod Bay with an extensive shoreline. Fishermen bring boats inside the 500-yard security zone. During the summer months, there is considerable pleasure boat traffic crisscrossing in front of the reactor site.

Pilgrim was one of seven nuclear plants identified as vulnerable to a ship-borne attack, in the 2013 Pentagon-contracted study "Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current 'Design Basis Threat' Approach" referenced above.

The primary concerns regarding water-borne attacks are using a boat as a floating or submerged explosive bomb delivery vehicle targeting the reactor or other key building onsite; and/or placing a charge up the intake canal to disrupt the cooling system; and using a boat as a commando transport vehicle.

Current Status: There is a 500-yard "exclusion zone," but it is simply marked by buoys – the equivalent of "no-trespassing signs." It is not impenetrable, and does not appear to be patrolled most of the time.

The Coast Guard patrols, but only occasionally since the Coast Guard's resources are limited. Once the patrol leaves the site, a terrorist can strike. A floating boom is, or was going to be, placed across the mouth of the intake canal but this will not stop a submerged weapon. The "exclusion" zone was breached many times – sunbathers, fishermen, kayakers. A large Norwegian sailboat anchored inside the exclusion zone overnight, with its lights on. Entergy called the Harbormaster but not until the following morning.

[12] Gerald L. Dillingham, US General Accounting Office, testimony before the Committee on Commerce, Science and Transportation, US Senate, "Aviation Security: Progress Since September 11, 2001, and the Challenges Ahead", 9 September 2003

Recommendations: Others have solved this perplexing security problem over open waters by training intelligent cameras i.e. long range thermal video detection cameras with intelligence built into the camera or built into the video head-end at the security monitoring and control location and the use of radar and sonar. One suite of a complete waterside security system might consist of the following:

- High Performance Swimmer Detection Sonar System
- Enhanced Capability Intrusion Detection Radar System
- CCTV, Low Light TV, IR Imaging System
- Command, Control, Communications and Display System
- Long range acoustic beams
- Waterborne sea fence-as used by the Department of Defense to protect anchored ships and nuclear submarines

Land-based security: *Owner Controlled Area, Protected Area,* and *Vital Area* are three key terms in nuclear plant security Most of the *Owner Controlled Area* around a nuclear power plant can be accessed by the public without special permission. The double-fenced perimeter surrounding some, but not all, of the buildings at a nuclear plant marks the Protected Area that requires prior authorization and badges to enter. Additional protection is provided by limiting access to Vital Areas within the Protected Area to only those workers specially authorized to enter them.

From July 2011 to September 2014, the press reported 10 trespassing events on to Pilgrim's owner-controlled area. The guard house is not manned, allowing access down the main driveway. Experts outside the NRC disagree with Entergy's and NRC's cavalier attitude. Dr. Edwin Lyman, a security expert at the Union of Concerned Scientists, explained[13] that a visible security presence is vital, because it may deter terrorists from targeting a facility in the first place. Lyman said:

> Part of security is to have a visible defense so that it doesn't attract adversaries who might see this kind of weakness to exploit … the industry has really let those owner-controlled areas protections just completely erode. And they're leaving the checkpoints unmanned all the time and not doing surveillance of the areas so people can enter the owner controlled area

[13] http://dailycaller.com/2014/09/08/thedc-investigates-lax-security-at-nuclear-power-plant-outside-washington-video/

without any problem or detection. And I think that's a problem… I think it's kind of foolish to allow such lax controls over the owner-controlled area.

Weapons: Reactors do not have to be prepared to protect against rocket-propelled grenades or 50-caliber sniper rifles, both readily available.

Cyber Attacks: NRC's backgrounder on cyber attacks[14] says that "Nuclear power facilities use digital and analog systems to monitor, operate, control, and protect their plants. "Critical digital assets" that interconnect plant systems performing safety, security, and emergency preparedness functions are isolated from the Internet. This separation provides protection from many cyber threats." Protection perhaps from many, but not all.

A paper prepared for the the Plymouth Nuclear Affairs Committee[15] provided a preliminary tutorial on cybersecurity and Pilgrim. The following draws from that analysis.

Pilgrim, along with other sites, may have integrated their control systems with computer networks built from off-the-shelf commercial operating systems, such as Windows and Unix. This has made process control systems more vulnerable to attack over the internet.

NRC and licensees used to believe that the process control systems were not vulnerable to attack because: They assumed that Process Contol Systems (PCS) were isolated from the internet; and PCS generally use proprietary protocols and hardware not compatible withordinary computers and common network protocols like Ethernet and TCP/IP.

The Plymouth analysis reported on three in-cyber attack incidents at US reactors. It said:

1. In 2003, the Slammer worm began exploiting vulnerability in Microsoft SQL servers. Within ten minutes, it had infected 75,000 servers worldwide—90% of vulnerable hosts. The design of Slammer was simple; it did not write itself to the hard drive, delete files, or obtain system control for its author. Instead, it settled in system memory and searched for other hosts to infect. Although Slammer carried no malicious payload, it still caused considerable disruption. It searched for new hosts by scanning random IP addresses. This generated a huge volume of spurious traffic, consuming bandwidth and clogging networks. The Slammer worm also infected computer systems at the Davis-Besse nuclear power plant. The worm traveled from a consultant's network, to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks, thus for four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS), which shows sensitive data about the reactor core collected from coolant systems, temperature sensors, and radiation detectors—these components would be the first to indicate meltdown conditions. Although Slammer's scanning traffic did block sensors from providing digital readouts to control systems, it did not affect analog readouts on the equipment itself; plant technicians could still get reliable data from sensors by physically walking up to them and looking at them, though this process is slower than retrieving data over a network. Davis-Besse also had a firewall protecting its corporate network from the

[14] http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/cyber-security-bg.html

[15] Cybersecurity and PNNP: a Preliminary Tutorial, Richard Grassie prepared for the Nuclear Matters Committee-Plymouth, Massachusetts, Monthly Meeting, Monday 19 January 2015

wider internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network, thereby inadvertently allowing Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network.

2. In 2006, a shutdown of Unit 3 at Browns Ferry nuclear plant occurred demonstrating that not just computers, but even critical reactor components, could be disrupted and disabled by a cyberattack. Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineralizer controller, both of which devices were a kind of programmable logic controller (PLC) where the recirculation pumps were dependent on variable frequency drives (VFD) to modulate motor speed. Both kinds of devices have embedded microprocessors that can communicate data over Ethernet yet both devices are prone to failure in high traffic environments. The Browns Ferry control network produced more traffic than the PLC and VFD controllers could handle and they failed.
3. In 2008, Unit 2 of the Hatch nuclear power plant automatically shut down after an engineer applied a software update to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks. When the engineer rebooted the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems.
4. The Stuxnet attack against the Iranian nuclear program demonstrates the impact that a sophisticated adversary with a detailed knowledge of process control systems can have on critical infrastructures. Stuxnet is believed to have destroyed 984 centrifuges at Iran's uranium enrichment facility in Natanz. The Stuxnet worm targeted specific PCS components used in the Iranian centrifuge cascades. The PLCs controlled the frequency converters to modulate the speed at which the centrifuges spun. Stuxnet commanded the PLCs to speed up and slow down the spinning centrifuges, destroying some of them, while sending false data to plant operators to make it appear the centrifuges were behaving normally. It was found that Stuxnet's authors may have learned about vulnerabilities in the Siemens controllers at another site in the US, thus making process control systems made up of Siemens controllers vulnerable.

   The Stuxnet attack also demonstrates elements of the other cyberattack incidents mentioned above. First, it disrupted the systems that monitored physical components, like the Davis-Besse worm infection. Second, it interfered with programmable logic controllers, like the Browns Ferry data storm. Third, it relied on there being some path from ordinary office computer to process control systems, as in the Hatch automatic shutdown. Moreover, it travelled between computers on worker's thumb drives and infected components prior to arrival along the various sources along the Iranian supply chain.

The Plymouth analysis took away from these examples the following:

1. First, skeptics claim that PCS are immune from attack since they are not connected to the internet. However, the Davis-Besse incident shows that this is a misconception, even operators who try to monitor and protect every connection cannot be sure they know about all of them. Stuxnet even traveled on portable thumb drives to infect computers that were not connected to the internet.

2. Skeptics argue that PCS are immune from attack since they are different from ordinary computers, however, all four incidents demonstrate that PCS have become interoperable with ordinary computers, making them vulnerable
3. Vulnerabilities are more complicated than both skeptics and alarmists realize. Alarmists often invoke the danger of hackers taking control of a power plant, but these incidents show how unintelligent computer viruses and even malfunctions in small devices can have big unexpected effects. This suggests that even though nuclear facilities are vulnerable to attack, a malicious hacker would have difficulty making sure an attack works precisely as planned.
4. States have developed significant knowledge and capabilities that make cyberattacks more precise, supplementing their methods with intelligence from other sources.

The report concluded that: In the absence of a workable, reliable and tested cybersecurity plan, PNPP has to be considered vulnerable along the same lines and in the same and possibly other manners mentioned for nuclear power plants above.

NRC Action or (in)action: All power reactor licensees must implement a cyber security plan under the NRC's cyber security regulations. (10 CFR 73.54) Despite the hype about cybersecurity following the North Korea attack on Sony for example, NRC gave Pilgrim an extension to provide its Cyber Protection Plan until June 30, 2016.

NRC Force-On-Force Tests Of Security

"Force-on-force" inspections of a nuclear power plant's security occur every three years. A team of mock terrorists test the ability of nuclear plant security forces to protect the plant from sabotage attacks that could cause a reactor meltdown or damage to spent fuel in storage pools. (Spent fuel stored in dry casks is not designated as a target for force-on-force tests: a big loophole.) These tests are important because having a good security plan on paper is not a guarantee that a plant security force could effectively carry out the plan in practice.

Dr. Edwin Lyman, Union of Concerned Scientists, explained[16]:

> The tests are intended to be as realistic as possible, but they have significant limitations. For one thing, they lack the element of surprise, which is one of the most critical tactical advantages of a real attacking force. A nuclear site must be notified well in advance of the inspection to ensure that security forces know that it is not a real attack and to give the plant management time to implement measures to maintain safety and security during the tests. However, the more advance notice the NRC provides, the more time and resources become available for plant management and security forces to prepare for the test, and the less representative the test will be of an actual surprise attack.
>
> In the force-on-force test program that was carried out in the 1990s, nuclear plants were given 6-12 months' advance notice, and plant managers spent hundreds of thousands of dollars getting ready. (Even so, about 50% of the plants failed the test.) But after the 9/11 attacks, when the program was revamped and strengthened, the NRC staff mandated that

[16] http://allthingsnuclear.org/elyman/ominous-votes-by-the-nrc; and file:///C:/Users/Mary/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/UED2GFA7/20160307-ucs-three-phase-power-backgrounder.pdf

the notification period should not be greater than 12 weeks because "a longer notification window might not provide as accurate an assessment of typical security force readiness."

But in a paper dated (perhaps inauspiciously) September 11, 2015[17], the staff proposed that the notification window be increased again to 9-15 months so that the inspections could be included in the regular periodic notice of all upcoming inspections that are sent to licensees, which according to the staff would "minimize disruptions to the NRC and licensees without impacting the integrity of the inspection program." And on October 6, the four sitting NRC commissioners voted unanimously to approve the change.

Now, if only the NRC could give 15 months advance warning for a real attack, we'd be all set.

For more on Force-on-Force tests see: http://allthingsnuclear.org/elyman/the-nrcs-security-inspections-at-nuclear-power-plants-are-again-under-attack?

VULNERABILITY PILGRIM'S DRY CASKS

Casks are vulnerable to attack: Pilgrim's casks will be lined up vertically on a pad, in the open and vulnerable to attack – an arrangement referred to as "candlepin bowling for terrorists." Casks are vulnerable from an air or land-based attack with weapons readily available today.[18] Despite their vulnerability, the NRC commissioners voted on September 11, 2015[19] to postpone the schedule for developing new requirements for protecting spent fuel in dry cask storage from sabotage by five years. There are a number of good reasons to implement this rule sooner. The most important one is that the current rules do not provide adequate protection of dry casks from certain types of terrorist attack scenarios, as the NRC has acknowledged publicly.

[17] http://pbadupws.nrc.gov/docs/ML1523/ML15231A232.pdf

[18] The Massachusetts Attorney General's Request for a Hearing and Petition for Leave to Intervene With respect to Entergy Nuclear Operations Inc.'s Application for Renewal of the Pilgrim Nuclear Power Plants Operating License and Petition for Backfit Order Requiring New Design features to Protect Against Spent Fuel Pool Accidents, Docket No. 50-293, May 26, 2006 includes a Report to The Massachusetts Attorney General On The Vulnerability of Pilgrim's Spent Fuel Pool- Risks and Risk-Reducing Options Associated with Pool Storage of Spent Nuclear Fuel at the Pilgrim and Vermont Yankee Nuclear Power Plants, Gordon Thompson, May 25, 2006;Environmental Impacts of Storing Spent Nuclear Fuel and High-Level Waste from Commercial Nuclear Reactors: A Critique of NRC's Waste Confidence Decision and Environmental Impact Determination, Dr. Gordon Thompson, February 6, 2009, pgs., 29, 47, 50, Tables 7-6, 7-7.

[19] http://allthingsnuclear.org/elyman/ominous-votes-by-the-nrc

Dr. Gordon Thompson analyzed the impact of the shaped charge as a potential instrument of attack.[20] The analysis shows that the cylindrical wall of the canister is about 1/2 inch (1.3 cm) thick, and could be readily penetrated by available weapons. The spent fuel assemblies inside the canister are composed of long, narrow tubes made of zirconium alloy, inside which uranium oxide fuel pellets are stacked. The walls of the tubes (the fuel cladding) are about 0.023 inch (0.6 mm) thick. Zirconium is a flammable metal.

Table 7-7:Performance of US Army Shaped Charges, M3 and M2A3

Target Material	Indicator	Type of Shaped Charge	
		M3	M2A3
Reinforced concrete	Maximum wall thickness that can be perforated	60 in	36 in
	Depth of penetration in thick walls	60 in	30 in
	Diameter of hole	• 5 in at entrance • 2 in minimum	• 3.5 in at entrance • 2 in minimum
	Depth of hole with second charge placed over first hole	84 in	45 in
Armor plate	Perforation	At least 20 in	12 in
	Average diameter of hole	2.5 in	1.5 in

Notes: (a) Data are from: Army, 1967, pp 13-15 and page 100.(b) The M2A3 charge has a mass of 12 lb, a maximum diameter of 7 in, and a total length of 15 in including the standoff ring. (c) The M3 charge has a mass of 30 lb, a maximum diameter of 9 in, a charge length of 15.5 in, and a standoff pedestal 15 in long.

[20] Gordon R. Thompson, *Environmental Impacts of Storing Spent Nuclear Fuel and High- Level Waste from Commercial Nuclear Reactors: A Critique of NRC's Waste Confidence Decision and Environmental Impact Determination* (Cambridge, Massachusetts: Institute for Resource and Security Studies, 6 February 2009). Tables also in Declaration of 1 August 2013 by Gordon R. Thompson: Comments on the US Nuclear Regulatory commission's Draft Consequence Study of a Beyond-Design-Basis Earthquake Affecting the Spent Fuel Pool for a US Mark I Boiling Water Reactor

Table 7-8: Types of Atmospheric Release from a Spent-Fuel-Storage Module at an ISFSI as a Result of a Potential Attack

Type of Event	Module Behavior	Relevant Instruments and Modes of Attack	Characteristics of Atmospheric Release
Type I: Vaporization	• Entire module is vaporized	• Module is within the fireball of a nuclear-weapon explosion	• Radioactive content of module is lofted into the atmosphere and amplifies fallout from nuc. explosion
Type II: Rupture and Dispersal (Large)	• MPC and overpack are broken open • Fuel is dislodged from MPC and broken apart • Some ignition of zircaloy fuel cladding may occur, without sustained combustion	• Aerial bombing • Artillery, rockets, etc. • Effects of blast etc. outside the fireball of a nuclear weapon explosion	• Solid pieces of various sizes are scattered in vicinity • Gases and small particles form an aerial plume that travels downwind • Some release of volatile species (esp. cesium-137) if incendiary effects occur
Type III: Rupture and Dispersal (Small)	• MPC and overpack are ruptured but retain basic shape • Fuel is damaged but most rods retain basic shape • No combustion inside MPC	• Vehicle bomb • Impact by commercial aircraft • Perforation by shaped charge	• Scattering and plume formation as for Type II event, but involving smaller amounts of material • Little release of volatile species
Type IV: Rupture and Combustion	• MPC is ruptured, allowing air ingress and egress • Zircaloy fuel cladding is ignited and combustion propagates within the MPC	• Missiles with tandem warheads • Close-up use of shaped charges and incendiary devices • Thermic lance • Removal of overpack lid	• Scattering and plume formation as for Type III event • Substantial release of volatile species, exceeding amounts for Type II release

One type of scenario for an atmospheric release from a dry cask would involve mechanical loading of the module in a manner that creates a comparatively small hole in the canister. The loading could arise, for example, from the air blast produced by a nearby explosion, or from the impact of an aircraft or missile. If the loading were sufficient to puncture the canister, it would also shake the spent fuel assemblies and damage their cladding. A hole with an equivalent diameter of 2.3 mm, radioactive gases and particles released would result in an inhalation dose (CEDE) of 6.3 rem to a person 900 m downwind

from the release. Most of that dose would be attributable to release of two-millionths (1.9E-06) of the MPC's inventory of radioisotopes in the "fines" category.

Another type of scenario for an atmospheric release would involve the creation of one or more holes in a canister, with a size and position that allows ingress and egress of air. In addition, the scenario would involve the ignition of incendiary material inside the canister, causing ignition and sustained burning of the zirconium alloy cladding of the spent fuel. Heat produced by burning of the cladding would release volatile radioactive material to the atmosphere. Heat from combustion of cladding would be ample to raise the temperature of adjacent fuel pellets to well above the boiling point of cesium.

Potential for Release from a Cask and Consequences: Dr. Thompson observes that**:** Casks are not robust in terms of its ability to withstand penetration by weapons available to sub-national groups. A typical cask would contain 1.3 MCi of cesium-137, about half the amount of cesium-137 released during the Chernobyl reactor accident of 1986. Most of the offsite radiation exposure from the Chernobyl accident was due to cesium-137. Thus, a fire inside an ISFSI module, as described in the preceding paragraph, could cause significant radiological harm.

Each cask contains ½ the Cesium-137 released at Chernobyl

Options to reduce risk: Use thick-walled metal casks, dispersal of the casks, and protection of the casks by berms or bunkers in a configuration such that pooling of aircraft fuel would not occur in the event of an aircraft impact.

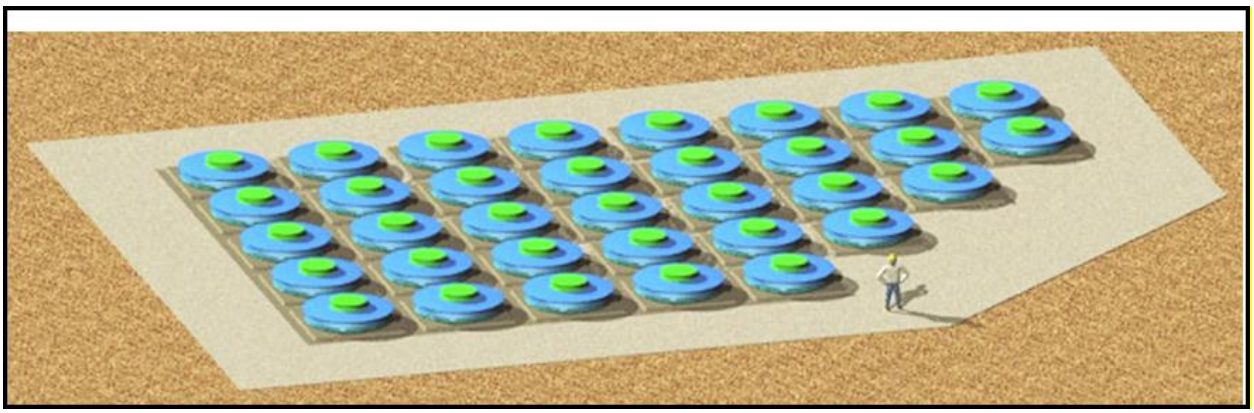
Holtec has developed a design for a new ISFSI storage module that is said to be more robust against attack than present modules. The new module is the HI-STORM 100U module, which would employ the same canister used in the present Holtec modules. For most of its height, the 100U module would be underground. Holtec has described the robustness of the 100U module as follows[21]:

> "Release of radioactivity from the HI-STORM 100U by any mechanical means (crashing aircraft, missile, etc.) is virtually impossible. The only access path into the cavity for a missile is vertically downward, which is guarded by an arched, concrete-fortified steel lid weighing in excess of 10 tons. The lid design, at present configured to easily thwart a crashing aircraft, can be further buttressed to withstand more severe battlefield weapons, if required in the future for homeland security considerations. The lid is engineered to be conveniently replaceable by a later model, if the potency of threat is deemed to escalate to levels that are considered non-credible today."

San Onofre is installing the HI-STORM 100U module. **Critics advise that** Holtec HI-STORM UMAX canister storage systems and other Holtec thin canister storage systems cannot be inspected, repaired, adequately monitored and have all the conditions for stress corrosion cracking. Canisters with cracks cannot be transported according to NRC Regulation 10 CFR § 71.85. **Further, it is** not practical to repair a damaged canister, says Dr. Kris Singh, CEO, Holtec International. To read a discussion of these casks, please visit

[21] Holtec International, "The HI-STORM 100 Storage System", accessed at <http://www.holtecinternational.com/hstorm100.html> on 17 June 2007.

http://sanonofresafety.org/holtec-hi-storm-umax-nuclear-waste-dry-storage-system/



http://www.holtecinternational.com/productsandservices/wasteandfuelmanagement/hi-storm/hi-storm-100u/

Liability – Who is responsible if there is a problem-Entergy or Holtec?

Casks will remain onsite for decades. If Holtec is liable, is the company arranged like Entergy with multi-tiered limited liability companies?

National Academies: Congress asked the National Academies to analyze the safety and security of commercial spent nuclear storage in the United States.[22] The report listed additional steps to be taken to make dry casks less vulnerable to reduce the liklihood of releases of radioactive material from dry casks in the event of a terrorist attack. The recommendations included:

- Additional surveillance could be added to dry cask storage facilities to detect and thwart ground attacks.
- Certain types of cask systems could be protected against aircraft strikes by partial earthen berms. Such berms also would deflect the blasts from vehicle bombs.
- Visual barriers could be placed around storage pads to prevent targeting of individual casks by aircraft or standoff weapons. These would have to be designed so that they would not trap jet fuel in the event of an aircraft attack.
- The spacing of vertical casks on the storage pads can be changed, or spacers (shims) can be placed between the casks, to reduce the likelihood of cask-to-cask interactions in the event of an aircraft attack.
- Relatively minor changes in the design of newly manufactured casks could be made to improve their resistance to certain types of attack scenarios."(Report, pg., 68)

[22] Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report, National Academies of Sciences, April 2005, http://www.nap.edu/books/0309096472/html/