Indian Point Safe Energy Coalition (IPSEC)
PO Box 131
Ossining, NY 10562-0131
1 (888) 474-8848

February 11, 2016

Comments of the Indian Point Safe Energy Coalition (IPSEC) on Nuclear Regulatory Commission (NRC) Rulemaking: Mitigation of Beyond-Design-Basis Events, Docket ID Nos: NRC–2014–0240; PRM-50-97 and PRM-50-98; NRC-2011-0189 and; RIN 3150-AJ49 (proposed consolidated rule which combines rulemaking for *Onsite Emergency Response Capabilities* and *Station Blackout Mitigation Strategies* NUREG-2157) dated Sep 2013

Secretary
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001
ATTN: Rulemakings and Adjudications Staff

Via e-mail Rulemaking.Comments@nrc.gov and Carol.Gallagher@nrc.gov with Supporting Sources Appendix sent via postal mail

Dear Nuclear Regulatory Commission:

The Indian Point Safe Energy Coalition (IPSEC) is a coalition of public interest, health advocate, environmental and citizen groups. We submit these Comments in regard to the referenced Mitigation of Beyond Design Basis Events rulemaking (a/k/a **Mitigation Rulemaking**).

PRELIMINARY STATEMENT

There is a great deal to commend in the referenced Mitigation Rulemaking. It clearly represents an enormous effort on the part of the team which devised it. Our Coalition is particularly relieved to finally see attention paid to station blackout (a/k/a SBO) and some recognition of the forces which Mother Nature is increasingly inclined to wield. We see little for objection with respect to the enhanced capabilities which the Mitigation Rulemaking seeks to establish.

However we do have strong concerns and objections regarding crucial omissions and exceptions in the proposed rule.

In consideration of your staff's time, we here focus on several broad schematic concerns and note only what we believe are the most serious flaws. The points raised are widely applicable to all reactor sites, but are especially relevant to plants located in populated regions. It is imperative the NRC begin to incorporate population demographics, plant operational history, and the risk of terror attack into both risk analysis and regulatory framework construct.

Indian Point warrants exceptionally heightened level of concern given the fact it is sits in the most densely packed and highest population area of any nuclear site in the nation and the fact that the New York City Metropolitan Area has been repeatedly targeted for terrorist action.

Indeed, as far as we are aware, Indian Point remains the only reactor site which has been specifically considered as a terror target.

The body of these Comments simply outlines key issues: four broad and four specific. More detailed information warranting attention is set forth in the accompanying Supporting Sources Appendix.

BROAD SCHEME CONCERNS

Industry Self-Regulation

The first schematic flaw – and it may unfortunately be a fatal one – is that the scheme remains effectively left to the industry to self design and implement. The problem with this should be self-evident.

Inadequate and Unelucidated Spectrum of Beyond Design Basis Scenarios

The second schematic flaw is a failure to delineate – and apparently to give consideration to – the many different accident initiator and exacerbator scenarios that the events of even just this new century have brought to light. It is well and good (although quite late) to begin implementation of the "Fukushima Lessons Learned." But many of the Chernobyl; 9/11; BP and Deepwater Horizon lessons appear quite forgotten, as do those of Katrina; Sandy and the long litany of other storms and natural and manmade disasters that have beset the U.S. in recent years – with the Flint Michigan contaminated water crisis being just the latest.

It is not just earthquakes, floods and loss of off-site power, but landslides; dam bursts; severe droughts; extreme storms; wildfires; and malevolent action conditions which must be considered. And such events in combination and/or in rapid succession over large geographic regions, with all the attendant chaos and infrastructure damage that would ensue, require serious consideration.

Most notably, nuclear power accidents occurring during natural and manmade disasters can involve the release of large quantities of radioactivity during periods when populations are simultaneously trapped and fleeing. Mitigation response may require thousands of responders to be active for prolonged periods. Such responders include the National Guard and Reservists; firefighters; federal state and local law enforcement; HAZMAT; construction workers; utility workers; large equipment operators; transit workers; public officials; public health workers; volunteer groups like the Red Cross; and large numbers of individual citizens. In fact, if there is one thing we know for a *certainty* from all of the recent disasters above noted, it is that responders are not just First Responders.

Indeed the responders and populations affected by the Fukushima disaster were not just those impacted during the active phase of the accident or even those under the multiple radioactive plumes released over months. Fukushima's damage extends to the many thousands who suffered permanent loss of their homes and jobs and communities. While the meltdown occurred in a relatively unpopulated region of Japan, Fukushima's damage extends to all the

workers who will be exposed to radiation and other hazards for decades going forward. Fukushima's legacy includes all the as yet not fully known effects of long-lived radionuclides in the ocean and groundwater that was and is and will perhaps continue to be released for many years to come.

At what point is mitigation appreciably not enough? Might the threshold not be reached if the effects negatively impact populations for decades or centuries?

At what point do the numbers of individuals potentially harmed by a damaged nuclear operation become untenable? Is it 1000? 10,000? 100,0000? 1,000,000? 10,000,000?

In this regard it bears mention that over 80% of the radioactive plumes from Fukushima blew out over the Pacific Ocean. The nation of Japan was saved by lucky winds.

Fallout from a major inland nuclear power plant accident was demonstrated in fact by the 1986 Chernobyl disaster. Radioactive fires at Chernobyl burned fiercely for nearly 10 days. Changes in wind direction and rainfall resulted in an uneven and spotty distribution of radionuclides that left some areas 300 miles from the reactor more contaminated than others 30 miles away. The Chernobyl disaster resulted in the permanent relocation of 300,000 people, the severe contamination of over 1000 square miles of land, and a sizable geographical region being deemed uninhabitable for centuries.

But at least Chernobyl was situated in a relatively unpopulated region.

At Indian Point, some 300,000 people live within 10 miles, about 1 million live within 20 miles, and over 17,000 live within 50 miles (not even accounting for those who commute into the area). There is no ocean over which lucky winds would dispense the plume. The plume would fall on heavily populated New York City metro area and the Hudson River.

Mitigation Is An Assumption

The third schematic flaw relates to the concept of mitigation. "Mitigation" is an elusive term with a wide spectrum of applicability. This problem runs like a weak thread weaved throughout the greater NRC regulatory scheme. However it is particularly problematic with respect to beyond design basis eventualities, since the existing aging fleet of nuclear plants was not designed to consider many of the stressors it increasingly confronts.

How and where in this scheme – or any other in the NRC regulatory framework – is there allowance for the likelihood that certain kinds of accidents are likely effectively *unmitigatable*? Prime among these would be a spent fuel pool fire.

Vague Metrics

The fourth schematic flaw is that the metrics of compliance or success are unarticulated.

This issue links strongly to the strong reliance on the industry itself being the primary devisor of mitigation modes.

SPECIFIC FLAWS

The most serious specific flaws of the Mitigation Rulemaking are the (1) grandfathering provisions which allow structures which would not be considered safe today to continue in operation; (2) disregard of grave national security risks – not just terrorist attack(s), but sabotage and cyber; (3) discounting of the dangers inherent in the high level nuclear waste; and (4) the near full disregard of the untenable risk presented by the spent fuel pools over a very long duration.

Recitation of facts pertaining to the fourth flaw should readily illustrate the risks inherent in the other three:

- Nuclear waste (spent fuel) is among the most hazardous materials on the planet.
- Nuclear waste remains highly toxic for hundreds of thousands of years.
- When the spent fuel pools were originally constructed they were planned to hold spent fuel for a very short term – less than a year. The spent fuel pool structures at nuclear plant sites were thus never designed, nor built, with the intention of holding large quantities of nuclear material for four decades, much less a near century.
- Nearly 70,000 metric tons of high-level nuclear waste are being stored at commercial nuclear power plants and the amount is expected to increase at a rate of approximately 2,000 a year or 20,000 MTU each decade.
- The typical spent fuel pool at a light water reactor now holds the equivalent of about 6 reactor core loads of spent fuel, about 700 MTU.
- Low-burnup fuel can be transferred from cooling pools into dry casks after 5 years, but high-burnup fuel may need to remain within pool cooling for 20 years or more, and the use of high-burnup fuel has been increasing. Further, aging effects/mechanisms applicable to high-burnup fuel remain to be determined
- America's existing nuclear fleet and the on-site spent fuel pools where most of the high-level spent fuel waste remains stored are aging.
- It is a fundamental of engineering that as machines and structures age they become subject to age-related deterioration and aging effects/mechanisms apply to spent fuel pools and their associated structures.
- Spent fuel pools at Indian Point and elsewhere have already shown evidence of age related deterioration and deterioration of fuel cladding.
- Climate change, with extreme weather, oscillating temperatures, and disturbed environmental dynamics render past analyses of component and structure performance outmoded. Basing estimation of performance based on "historic" data of weather or ambient conditions is no longer valid.

- Unlike the reactors, the spent fuel containments are not hardened. The roofs are similar to the roofs commonly built at box top stores.

- Accidental releases of radiation into environment from spent fuel pools have already occurred at Indian Point and at other nuclear plant sites.

- Attestations as to the safe containment of large quantities of nuclear waste – particularly high burnup fuel – in spent fuel pools for half a century or beyond are hypothetical, based on limited collections of experiential data, and untested by reality.

- Security and nuclear experts have identified spent fuel pools to be non-robust terrorist targets, vulnerable to tactics such as kamikaze aircraft strikes and demolition of cooling intake structures via MANPADs or targeting with explosive laden speedboats.

And yet the Mitigation Rulemaking proposes allowance of relaxation of emergency planning and capability for spent fuel pools?

This is a stupendously reckless proposal.

It also flies in the face of the Mitigation Rulemaking's purported goal which is to increase protection with regard to beyond design basis events.

While it is reasonable to reduce requirements for some dormant and unused plant structures following decommissioning, it is unacceptable to lower any safeguard of spent fuel pools. To the contrary, the combined effects of aging and climate change stressors mandate increased oversight.

As decades go by these old deteriorated structures will become more and more vulnerable to natural disasters and other high-load events.

Spent fuel pools at sites proximate to active seismic faults have especially elevated risk, since the geometry of both the pools and the landscape (including the rock and soil structural foundation) can be dramatically altered. Cooling water supply pipes can rupture, debris can collapse (displacing cooling water), and the pool walls can crack. Notably, at Indian Point, a considerable portion of one of the pool structures is buried and inaccessible to full inspection. Even moderately compromise of containment could lead to a long-term leaking/leaching of radioactive water into the groundwater and nearby source water. This would be a slow-forming radiation disaster similar to that which Fukushima's underground leaking may portend. The end result could be a kind of radioactive version of the Flint, Michigan contaminated water disaster.

Sites proximate to hazard-elevating non-nuclear infrastructure such as high-pressure pipelines must also be understood to pose elevated risk mandating far more protection than now envisioned.

Indian Point, for example, has had more than 10 fires already, the most recent from a transformer explosion in May 2015 which additionally led to a leak of 20,000 gallons of oil into the Hudson River. The fire was able to be fought without radioactivity release because the transformer did not hold radioactive elements. Such would not be the case in an effort to fight a

containable fire threatening the spent fuel pools since the overflow of cooling water would distribute substantial radioactivity.

Of more concern is a sudden explosion-triggered fire and the risks here extend way past decommissioning. At Indian Point, for example, two half-century-old interstate natural gas lines currently run mere yards from the site. One gas line is 30" in diameter, the other is 26". The lines are part of a system that transports some 2.4 billion cubic feet of gas at high pressure every day. Adding considerably to the hazard of a gas explosion and fire, is the recent approval of a third pipeline: the Spectra Energy Algonquin Incremental Market Project pipeline (or AIM Pipeline), a 42-inch high-pressure gas pipeline planned for construction right next to the nuclear site. The rupture of a gas pipeline of the AIM size could release explosive gas at the rate of 376,000 kilotons (nearly 1 million pounds) per minute, experts warn. (More detail is recited in the Appendix to these Comments.) The blast and fire radius could readily encompass spent fuel pool structures.

The fact that spent fuel may be somewhat less hot after sitting in a pool for many years may reduce the risk of spontaneous fire, but it hardly protects against a massive gas explosion and inferno that could engulf the entire facility. Planes (even small planes) laden with fuel or explosives crashing into the roofs of a spent fuel pool structure would likewise potentially ignite a catastrophic spent fuel fire. And, as many nuclear experts have pointed out, a spent fuel pool fire would emit extraordinarily high levels of radioactivity, making extinguishment all but impossible.

CONCLUSION

The American people are now stuck with aging nuclear plants and a virtual continuous litany of "events" and "incidents" at nuclear plant sites. Of particular concern are the massive quantities of high level nuclear waste sitting in spent fuel pools, perhaps in perpetuity. The NRC should – at the very least – require operators of commercial nuclear power plants to provide the strongest possible storage for nuclear fuel; both new and spent for as long as communities are put at risk by these nuclear materials.

Safeguards need to be commensurate with the risk and high level nuclear waste remains highly hazardous under decommissioning and long-term conditions.

The NRC disregards the strong likelihood that climate change will exert a multiplier effect on the aging mechanisms applicable to spent fuel assemblies and spent fuel pools.

For a wide assortment of risks – flooding risk, dam failure risk, earthquake risk, site structure hazard risk, construction accident risk, landslide risk, hurricane risk, tornado risk, site fire risk, wildfire risk, malevolent insider risk, terrorism risk, human error, acts of nature, you name it – small risks can grow pretty exponentially when combined and when the time periods are long.

The safety, security, health and environmental dangers involved in nuclear power are of such potential magnitude that neither the commercial nuclear industry, nor the insurance industry, has been willing to accept more than a fraction of the potential liability. Industry lobbying has enabled laws like the Price-Anderson Act of 1957 and the Nuclear Waste Policy Act of 1982 to shift the substantial risk burden to the American citizenry and taxpayers.

The NRC continues to allow nuclear power plants to be owned and run by limited liability corporations and other legal constructs which would allow the multi-billion parent corporations to walk away from a major liability, not just in the future, but today.

The commercial viability of the nuclear power industry may not properly be weighed against the continued viability of communities, the health welfare and safety of tens of millions of Americans, and the habitability of sizable regions of the nation for generations to come.

We applaud efforts to tackle the challenges and exigencies which may arise under nuclear plant emergency conditions and are glad to see more attention paid to improving emergency response and integrating reaction capability. Reevaluation of station blackout conditions, manpower, training, equipment, site condition monitoring, off-site radioactive release monitoring, communication systems... all of these steps are positive and long overdue.

But enhanced coping capability does not alone provide a level of assurance a disaster will not be a disaster.

Sincerely,

Michel Lee, Esq.
On behalf of the Indian Point Safe Energy Coalition

February 11, 2016

SUPPORTING SOURCES APPENDIX: INDIAN POINT SAFE ENERGY COALITION

Appendix to February 11, 2016 Comments of the Indian Point Safe Energy Coalition (IPSEC) on Nuclear Regulatory Commission (NRC) Rulemaking: Mitigation of Beyond-Design-Basis Events, Docket ID Nos: NRC–2014–0240; PRM-50-97 and PRM-50-98; NRC-2011-0189 and; RIN 3150-AJ49 (proposed consolidated rule which combines rulemaking for *Onsite Emergency Response Capabilities* and *Station Blackout Mitigation Strategies* NUREG-2157) dated Sep 2013

SUPPORTING SOURCES

Allison, Graham, *Nuclear Terrorism: The Ultimate Preventable Catastrophe*, Times Books Henry Hold and Company, LLC (2004).
https://ahmadishaq.files.wordpress.com/2014/05/1-nuclear-terrorism.pdf. See also http://www.coedat.nato.int/publication/datr/volume5/06-Nuclear_Terrorism_The_Ultimate_Preventable_Catastrophe.pdf.

[Allison Graham is a professor of government and Director of the Belfer Center for science and International Affairs at Harvard's John F. Kennedy School of Government, former Assistant Secretary of Defense for Policy and Plans (under Clinton), and former Special Advisor to the Secretary of Defense (under Reagan). This volume extensively describes terrorist agendas and black market dealings, and focuses substantially on the threat of radioactive ("dirty") bombs. A

10-kiloton nuclear bomb, delivered to Times Square by truck and then detonated, could kill up to one million New Yorkers.

A major concern of the American national security community in the weeks following 9/11, Graham says, was the so-called "second shoe" question – the question of what might happen next, when, where, and in what form.

"The American Airlines flight that struck the North Tower of the World Trade Center could just as readily have hit the Indian Point nuclear power plant, forty miles north of Times Square. The United Airlines flight that crashed in Pennsylvania on its way to the Capitol might instead have targeted Three Mile Island. The airplane that attacked the Pentagon could have targeted the North Anna power plant near Richmond, Virginia." A successful attack on a nuclear reactor could cause a meltdown releasing hundreds of times the amount of radioactivity as the Hiroshima and Nagasaki bombs. "An even more vulnerable target at a nuclear plant is the building that houses the spent fuel rods … these structure are open to the air in some instances and housed in only light-duty buildings in others, which means that a plane attacking from above might drain the pool, destroy backup safety systems, and ignite the fuel." (Introduction) As ret. Army Gen. and former counterterrorism chief Wayne Downig, told the Washington Post, "'"These guys continue to go back after targets they have tried to get before. That's why I expect they're going to go back to Washington and New York."'" (p 204)]

ARGONNE NATIONAL LABORATORY: Billone MC, Burtseva TA, Han Z and Liu YY, Effects of Multiple Drying Cycles on High-Burnup PWR Cladding Alloys, Argonne National Laboratory Study for Department of Energy, FCRD-UFD-2014-000052 ANL-14/11, Sep 26, 2014. http://www.ipd.anl.gov/anlpubs/2014/09/107521.pdf.

[High-burnup (HBU) fuel cladding "is subject to higher tensile hoop stresses induced by higher temperatures and pressure relative to in-reactor operation and pool storage." The high-burnup cladding alloys have a wide range of hydrogen contents. High-burnup cladding alloys also evidence varying hydride morphology after fuel removal from nuclear reactor cores.

There is a "lack of data for HBU fuel cladding after more than 20 years of storage, which corresponds to peak cladding temperatures of ≈200°C or less." (p 1)

"A major concern is whether or not HBU fuel will maintain cladding integrity and be readily retrievable after more than 20 years of storage." (p 1)

One of the "high priority activities is to establish the materials properties of cladding, especially for HBU cladding, and to supply models with the data necessary to determine how fuel rods will behave under normal, off-normal, and accident conditions, during both extended storage and transportation." (p 32)]

ARGONNE NATIONAL LABORATORY: Billone, 2012: Billone MC, Burtseva TA, and Yan Y, Ductile-to-Brittle Transition Temperature for High-Burnup Zircaloy-4 and ZIRLO™ Cladding Alloys Exposed to Simulated Drying-Storage Conditions, Report of Argonne National Laboratory, Sep 28, 2012. http://pbadupws.nrc.gov/docs/ML1218/ML12181A238.pdf.

[Compared to lower burnup rods, “high-burnup fuel rods are characterized by increased: decay heat following reactor discharge, internal gas pressure, cladding corrosion layer thickness, and cladding hydrogen content.” Authors conclude additional data will be needed to determine ductile-to-ductile transition temperature. However the trend of the data indicates that failure criteria for high-burnup cladding need to include the embrittling effects of radial-hydrides.]

ARGONNE NATIONAL LABORATORY and US DEPARTMENT OF ENERGY: Tsai H, Liu YY, Nutt M, and Shuler J, Advanced Surveillance Technologies for Used Fuel Long-Term Storage and Transportation, Proceedings of the 14th International Conference on Environmental Remediation and Radioactive Waste Management, Reims, France, ICEM2011, Sep 25-29, 2011.
https://inis.iaea.org/search/searchsinglerecord.aspx?recordsFor=SingleRecord&RN=43068395.

[Paper authored by scientists from the Argonne National Laboratory and the U.S. Department of Energy notes the “prospect looming for extended long term storage – possibly over multiple decades – and deferred transport, condition-and performance-based aging management of cask structures and components is now a necessity that requires immediate attention. From the standpoint of consequences, one of the greatest concerns is the rupture of a substantial number of fuel rods that would affect fuel retrievability.” Used fuel cladding – especially for high burnup fuels – may become susceptible to rupture due to radial-hydride-induced embrittlement caused by water-side corrosion during the reactor operation and thereafter. (p 1)

Air and moisture could also cause the zirconium-based fuel rod cladding to oxidize if the system temperature is sufficiently elevated. (p 2)

For high-burnup fuels, “there is presently insufficient data to confidently project rod integrity beyond even the short term.” (p 7)]

ASSOCIATED PRESS: Bryan, Susan Montoya and P Solomon Banda, Los Alamos Lab Under Siege From Wildfire, Associated Press, Jun 29, 2011.
http://www.pntonline.com/2011/06/28/los-alamos-nuclear-lab-under-siege-from-wildfire/.
[A 93 square mile wildfire advanced on the Los Alamos laboratory and thousands of outdoor drums of plutonium-contaminated waste June 28, 2011, as authorities stepped up efforts to protect the site and monitor air for radiation. As of midday, flames were as close as 50 feet from the lab grounds. A small patch of land at the lab caught fire June 27, but was quickly put it out. "‘We are throwing absolutely everything at this that we got,’ Democratic Sen. Tom Udall of New Mexico said in Los Alamos.”

The fire forced the evacuation of the entire city of Los Alamos, population 11,000, and cast “giant plumes of smoke over the region” raising fears among nuclear watchdogs that it might reach as many as 30,000 55-gallon drums of plutonium-contaminated waste. Joni Arends, executive director of the Concerned Citizens for Nuclear Safety said the the concern is that the drums could get so hot they'd burst or that fire could stir up nuclear-contaminated soil on lab property. As of midday June 28, flames were about two miles from the waste material. The lab has been shut down all week because of the fire.

Investigators do not know what sparked the fire, but suspicion has fallen on downed power lines.]

ASSOCIATED PRESS: Kole, William J, Global Atomic Agency Confesses Little Can Be Done to Safeguard Nuclear Plants, Associated Press, Sep 19, 2001. http://web.archive.org/web/20041025111540/http://www.nci.org/01/09/19-11.htm.

[At its annual conference, the International Atomic Energy Agency (IAEA) admitted that little can be done to shield a nuclear facility from a direct hit by an airplane. Most nuclear power plants were built during the 1960s and 1970s. IAEA spokesman David Kyde said: "'If you postulate the risk of a jumbo jet full of fuel, it is clear that their design was not conceived to withstand such an impact.'" An American official who declined to be identified, acknowledged that a direct hit at high speed by a modern jumbo jet full of fuel could create a Chernobyl situation.'"]

BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS AT HARVARD UNIVERSITY and INSTITUTE FOR U.S. AND CANADIAN STUDIES INSTITUTE OF THE RUSSIAN ACADEMY OF SCIENCES: Bunn M, Morozov CY, Mowatt-Larssen R, Saradzhyan, Tobey William, Yesin VI, and Zolotarev PS, The U.S.-Russia Joint Threat Assessment On Nuclear Terrorism, Joint Report of the Belfer Center for Science and International Affairs at Harvard University and the Institute for U.S. and Canadian Studies Institute of the Russian Academy of Sciences, May 2011. http://belfercenter.hks.harvard.edu/files/Joint-Threat-Assessment%20ENG%2027%20May%202011.pdf.

[International group of security and military experts warns nuclear terrorism is a real and urgent threat. Terrorists will certainly be searching for the "weakest link" in an otherwise well-defended nuclear establishment. "Moreover, the dramatic developments associated with the Fukushima disaster might awaken terrorist interest in this path to nuclear terrorism." (p 20)

"One important lesson of the Chernobyl and Fukushima accidents is that what can happen as a result of an accident can also happen as a result of a premeditated action. Indeed, today's high levels of nuclear safety are dependent on the high reliability of components such as cooling systems; if these are intentionally destroyed, the probability of a large release would increase greatly." (p 20)

"Overfilled spent fuel pools may also be potential sabotage targets; in some cases, if terrorists managed to drain the cooling water – as occurred without human intervention at Fukushima – a zirconium fire and large-scale dispersal of radioactivity could potentially result." (p 21)]

Brenner, Joel, "America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare," Penguin Press, New York (2011).

[Joel Brenner, served as head of counterintelligence for the U.S. Director of National Intelligence, and before that, as Inspector General of the National Security Agency. The book

exhaustively details and appraises the cybersafety and cybersecurity risks to the nation. The book reveals intrusions into the Pentagon, NASA, national laboratories, national infrastructure systems, and numerous corporate giants including major engineering, internet and computer security firms. Chapter 5, “Dancing in the Dark” (pp 93-115) describes nuclear plant and electrical grid vulnerability.]

BULLETIN OF THE ATOMIC SCIENTISTS: Alvarez R, What about the Spent fuel? Bulletin of the Atomic Scientists (2002); 58 (1): 45-47. http://www.nirs.org/radwaste/atreactorstorage/alvarezarticle2002.pdf.

[Robert Alvarez, is a former Senior Advisor to the U.S. Secretary of Energy.

While concerns about attacks on commercial nuclear power plants have focused mainly on the vulnerability of reactor containment buildings, spent fuel pools are a “weaker link”. On average, spent fuel pools hold 5 to 10 times more long-lived radioactivity than a reactor core, with the large amount of cesium 137 being particularly worrisome. “According to the NRC, as much as 100 percent of a pool’s cesium 137 would be released into the environment in a fire.” In comparison, the 1986 Chernobyl accident released only 40% percent of the core’s 6 million curies of C-137. “A single spent fuel pond holds more cesium 137 than was deposited by all atmospheric nuclear weapons tests in the Northern Hemisphere combined.”

“In 1982, the NRC’s Atomic Safety and Licensing Board ruled that reactor owners ‘are not required to design against such things as…kamikaze dives by large airplanes. Reactors could not be effectively protected against such attacks without turning them into virtually impregnable fortresses at much higher cost.’ This view is buttressed by NRC’s long-standing policy blocking consideration of terrorist attacks in licensing proceedings. Because acts of terrorism are unpredictable, the NRC reasons, they are not germane to safety requirements.”

“Equipment installed to make high-density ponds safe actually exacerbates the fire danger, particularly with aged spent fuel. In high-density pools at pressurized water reactors, fuel assemblies are packed about nine to 10.5 inches apart –slightly more than the spacing inside a reactor. To compensate for the increased risk of criticality, pools have been retrofitted with enhanced water chemistry controls and neutron-absorbing panels between assemblies. The extra equipment restricts water and air circulation, creating vulnerability to systemic failures. If the equipment collapses or fails, as might occur during a terrorist attack, for example, air and water flow to exposed fuel assemblies would be obstructed, causing a fire, according to the NRC report. Heat would turn the remaining water into steam, which would interact with the zirconium, making the problem worse by yielding flammable and explosive hydrogen. As a result, the NRC concluded that ‘it is not feasible, without numerous constraints, to define a generic decay heat level (and therefore decay time) beyond which a zirconium fire is not physically possible.’”

In June 2001 the NRC staff reported that terrorist threats against spent fuel pools are credible and cannot be ruled out “‘Until recently, the staff believed that the [design basis threat] of radiological sabotage could not cause a zirconium fire. However, [NRC’s safety policy for spent fuel storage] does not support the assertion of a lesser hazard to the public health and safety, given the possible consequences of sabotage.’”]

CENTER FOR PUBLIC INTEGRITY: Stranahan, Susan Q, Could rupture of aging pipeline ignite nuclear plant's control room? Less-noticed danger said to lurk near Indian Point reactor: high-pressure natural gas pipelines built half-century ago, Center for Public Integrity, May 11, 2014.
http://www.publicintegrity.org/2011/05/11/4544/could-rupture-aging-pipeline-ignite-nuclear-plants-control-room.

[The Indian Point nuclear power plant sits astride two active seismic zones for which it wasn't designed, and the probability of earthquakes was revised upward in 2014. It is a potential terrorist target and, over the years, the plant has been the scene of oil spills and radiation leaks. The lesser-known, but more likely threat is from two half-century old interstate natural gas lines which run about 200 yards (620 feet) from the Unit 3 reactor containment building. One gas line is 30" in diameter, the other is 26". The lines are part of a system that transports some 2.4 billion cubic feet of gas at high pressure every day.

"A rupture in one of those lines could create what one nuclear industry veteran familiar with the plant's operations called "'an 800-foot blowtorch.'" He said the inferno could render the control room uninhabitable and make it impossible to shut down Unit 3 — assuming operators survived the fire or, worse, an explosion." (The source requested anonymity for fear of retaliation.)
The danger of aging gas lines has been underscored by accidents in recent years. In San Bruno, Calif., a 30" gas line about as old as the lines at Indian Point The ruptured, exploded, and engulfed a neighborhood in flames, killing 8. In Edison, NJ, in 1994, a segment of interstate pipeline blew up, setting off a huge fire and destroying buildings.

Indian Point was chosen as a reactor site in 1955, when commercial nuclear power was in its infancy. In 1973, the U.S. Atomic Energy Commission, predecessor to the NRC, considered water-borne hazards and noted that the plant operator (then Con Ed), "'has indicated that no river traffic shipment of toxic materials or explosives currently pass the site.'"

Paul M. Blanch, an engineer who once worked as a consultant at Indian Point, has raised concern about the pipeline risk. The NRC dismissed these concerns in an April 2010 letter to Blanch. The NRC's determination is based on an August 2008 assessment made by the reactor operator, Entergy, which is not available to the public for independent review because — as the NRC notes — "'it contains security-related information.'"

The danger of gas lines close to a reactor has worried the NRC elsewhere, however. In 1991, the NRC determined that a rupture in a 16" low-pressure natural gas pipeline could pose a threat to a nuclear reactor — even though the reactor, in a sparsely populated area of Colorado, had been shut down for 2 years.

At Indian Point, regulators assumed automatic shutoff valves would protect the plant. But those valves were difficult to maintain. At some time prior to 1995, Blanch said, they were removed.]

CHATHAM HOUSE ROYAL INSTITUTE OF INTERNATIONAL AFFAIRS: Baylon C, Livingstone D, and Brunt R, Cyber Security at Civilian Nuclear Facilities: Understanding the Risks, Chatham House, the Royal Institute of International Affairs report summary,

Oct 5, 2015.
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf.

[Chatham House, the Royal Institute of International Affairs, is an independent policy institute based in London. Caroline Baylon is a science, technology and cyber security researcher at the Chatham's International Security Department; David Livingston is an Associate Fellow; and Roger Brunt is a nuclear security consultant.

The report concludes: "The risk of a serious cyber attack on civilian nuclear infrastructure is growing, as facilities become ever more reliant on digital systems and make increasing use of commercial 'off-the-shelf' software". The trend to digitalize, combined with a lack of executive awareness of the risks, "means that nuclear plant personnel may not realize the full extent of their cyber vulnerability and are thus inadequately prepared to deal with potential attacks."

Specific findings of the report:

- The contention that nuclear facilities are "air gapped" (isolated from the internet) is "a myth." Commercial benefits of internet connectivity has resulted in a number of nuclear facilities having virtual private network (VPN) connections – of which nuclear operators are sometimes unaware.
- Search engines readily identify critical infrastructure components with VPN connections.
- Even in air gapped nuclear plants, the safeguard "can be breached with nothing more than a flash drive."
- Equipment used at nuclear facilities is at risk of compromise at any stage because of supply chain vulnerabilities.
- Communication breakdowns between engineers and security personnel and inadequate training often leave nuclear plant personnel lacking understanding of key cyber security procedures.
- "Reactive rather than proactive approaches to cyber security contribute to the possibility that a nuclear facility might not know of a cyber attack until it is already substantially under way."]

CNN: Russia attacks U.S. oil and gas companies in massive hack, CNN Money, Jul 2, 2014. http://money.cnn.com/2014/07/02/technology/security/russian-hackers/

[Security firm Symantec report describes how hackers have sneaked malware into computers at gas pipeline companies and industrial equipment makers. Malware has also been identified inside the networks of universities doing research in the field of nuclear energy.]

Criscione, Lawrence S, PE and Paul M. Blanch, PE, Letter to Senator Joseph Lieberman, Chairman U.S. Senate Committee on Homeland security & Governmental Affairs, Dec 18, 2012. http://www.state.nv.us/nucwaste/news2012/pdf/criscione121218jlieberman.pdf.
[Lawrence Criscione is a risk engineer at the Nuclear Regulatory Commission headquarters in Maryland, and Paul Blanch is a nuclear engineer, NY nuclear safety consultant, and former employee at the Indian Point nuclear power plant in NY. In this letter they warn of dam break

risk to the Oconee Nuclear Station (S. Carolina) and gas pipeline rupture, explosion and fire risk to Indian Point (NY).]

ECOLOGICAL MONOGRAPHS: Evangeliou N, Balkanski Y, Cozic A, Hao WM, Mouillot F, Thonicke K, Paugam R, Zibtsev S, Mousseau TA, Wang R, Poulter B, Petkov A, Yue C, Cadule P, Koffi B, Kaiser JW, and Møller AP, Fire evolution in the radioactive forests of Ukraine and Belarus: future risks for the population and the environment, Ecological Monographs (2015); 85 (1): 49–72. Abstract. http://dx.doi.org/10.1890/14-1227.1

[International team of scientists are from the Institut Pierre et Simon Laplace, Laboratoire des Sciences du Climat et de l'Environnement (LSCE) (France); Missoula Fire Sciences Laboratory, Rocky Mountain Research Station Forest Service (US); Université Paul-Valéry Montpellier (France); Potsdam Institute for Climate Impact Research (PIK) (Germany); King's College London (UK); National University of Life and Environmental Sciences of Ukraine (Ukraine); University of South Carolina (US); Laboratory for Earth Surface Processes, College of Urban and Environmental Sciences, Peking University (China); European Commission, Joint Research Centre, Air and Climate Unit (Italy); European Centre for Medium-range Weather Forecasts (UK); Max-Planck-Institute für Chemie (Germany); and Laboratoire d'Ecologie, Systématique et Evolution (France).

Study analyzes current and future status of Ukraine and Belarus forests contaminated after the Chernobyl 1986 nuclear disaster and the risk of long-lived radiation spread due to forest fires. "Field measurements and modeling simulations confirmed that numerous radioactive contaminants are still present at these sites in extremely large quantities."

Authors' conclusion: "We predict that an expanding flammable area associated with climate change will lead to a high risk of radioactive contamination with characteristic fire peaks in the future."

Using several models, together with remote-sensing data and observations of conditions such as past forest fire activity, the scientific team also looked at how climate change in the forests could impact fire risk. Three scenarios of cesium- 137 (Cs^{137} or ^{137}Cs) displacement over Europe are postulated, each uses the assumption that 10% of forests were affected by fires. Differences derived on different emission altitudes of Cs^{137}.

"Forests in Eastern Europe are characterized by large, highly fire-prone patches that are conducive to the development of extreme crown fires. Since 1986, there has been a positive correlation between extreme fire events and drought in the two contaminated regions. Litter carbon storage in the area has doubled since 1986 due to increased tree mortality and decreased decomposition rates; dead trees and accumulating litter in turn can provide fuel for wildfires that pose a high risk of redistributing radioactivity in future years. Intense fires in 2002, 2008, and 2010 resulted in the displacement of ^{137}Cs to the south; the cumulative amount of ^{137}Cs re-deposited over Europe was equivalent to 8% of that deposited following the initial Chernobyl disaster. However, a large amount of ^{137}Cs still remains in these forests, which could be remobilized along with a large number of other dangerous, long-lived, refractory radionuclides."

"We predict that an expanding flammable area associated with climate change will lead to a high risk of radioactive contamination with characteristic fire peaks in the future. Current fire-fighting infrastructure in the region is inadequate due to understaffing and lack of funding. Our data yield the first cogent predictions for future fire incidents and provide scientific insights that could inform and spur evidence-based policy decisions concerning highly contaminated regions around the world, such as those of Chernobyl."]

ENERGY MATTERS: Witherspoon, Roger, NRC Probes Indian Point Security, Energy Matters, Nov 21, 2013. http://spoonsenergymatters.wordpress.com/2013/11/21/are-terrorists-training-at-nuclear-plant-nrc-probes-indian-point-security/.

[Reporting on serious security lapses at Indian Point: "Records show that for more than a decade, official at Indian Point have largely ignored instances where their internal security communications system was compromised and blocked by outside individuals. Whether the deliberate jamming of security communications is a decade-long prank or the result of individuals or groups using Indian Point safety drills as opportunities to test their own ability to cause mayhem during a terrorist attack is not known." Deliberate jamming was first reported in 2003 by James Lee Witt in an analysis of emergency planning for New York State. The problem forced cancellation of emergency drills in November 2012.

"Indeed, those who have hacked into Indian point's security have lately become so brazen that they have recorded instructions made by plant security officials at the beginning of drills, and then jammed the network's receivers by replaying those instructions over and over, according to participants, thus blocking any further use of the compromised security network. And the electronic intruders were apparently operating within a mile or two of the plant site."

Allegations of security failures at Indian Point have been made in a suit filed by two former security officers – Lt. Skip Travis and Lt. Jason Hettler –filed in U.S. District Court in August 2013 against Entergy include:

- "The falsification of work logs and fitness for duty reports, thus allowing security personnel to exceed the maximum permitted work hours per week despite being fatigued.
- "Jeopardizing the effectiveness of Force on Force drills by informing the security personnel of what routes the "invaders" would take to attack the plant.
- "A faulty perimeter detection system, which made it impossible for defenders to know where "terrorists" were breaking into the plant site and where they were on the grounds. As a result of being technologically blind during a drill monitored by the NRC on October 11, 2011, the suit states "all of the 'terrorists' successfully breached the perimeter and the identified target sets located inside of Indian Point and succeeded in causing a total nuclear meltdown. Not one terrorist was killed by any security personnel during the drill."
- "A combination of faulty detection equipment and internal communications allowed "terrorists" to succeed in in reaching all of their targets in an NRC-monitored, Force on Force drill in April, 2013. Hettler and Travis contend that had the April drill "been an actual terrorist attack, the 20 million individuals who live and work in the 50-mile radius meltdown zone would have perished."
- "An absence of backup power for the internal communications system. As a result, the security force could not communicate during station blackout conditions."]

Ferguson, Charles D and William C. Potter, "The Four Faces of Nuclear Terrorism," Routledge Taylor & Francis Group, New York and London (2005).

[Book by Charles D. Ferguson, Science and Technology Fellow at the Council on Foreign Relations, and William C. Potter, Institute Professor and Director of the Center for Nonproliferation Studies at the Monterey Institute of International Studies, also had contributors Amy Sands, Leonard S. Spector and Fred L Wehling of The Center for Nonproliferation Studies. The Forward by Richard G. Lugar, Chairman, U.S. Senate Foreign Relations Committee and Sam Nunn, Co-Chairman and Chief Executive Officer of the Nuclear Threat Initiative, notes "more likely terrorism dangers come from attacks on nuclear facilities...not designed to resist the level of terrorist threat that materialized on September 11"and that spent fuel pools are among the facilities "with weaker levels of or nonexistent containment structures."

Among "the nuclear facilities of greatest concern as potential terrorist targets" are those with significant inventories of radioactivity, including nuclear power reactors and "spent fuel storage facilities at these reactor sites". (p 190) The authors review the vulnerabilities of commercial nuclear plants in detail. (See, esp. pp 210-258) and specifically address issues identified at Indian Point.

"Attack modes include airplane crashes; commando raids by land, water, or air; or cyberterrorism." (p192) In the case of aerial attack, terrorists could precisely target "vital plant safety systems" such as the reactor's "spent fuel pools in order to generate substantial off-site release of radioactivity." (p 194) "If a terrorist attack or sabotage caused the spent fuel to be uncovered, its zirconium cladding might ignite, which might result in the release of radioactivity. The dense packing in most U.S. spent fuel pools restricts cooling flow, increasing the risk that temperatures could climb to high levels in the event that the spent fuel becomes uncovered." (p 205)]

Glickman, Dan and Harris Sherman, Paying for the Forest Fire Next Time, New York Times Op-Ed, Jun 18, 2014. http://www.nytimes.com/2014/06/18/opinion/paying-for-the-forest-fire-next-time.html.

[Dan Glickman was the secretary of the Agriculture Department from 1995 to 2001. Harris Sherman was the under secretary overseeing the Forest Service from 2009 to 2013.

Major fires are ravaging landscapes in California, Arizona, New Mexico and Alaska. Many wildfires have grown in heat, intensity and size in recent years, consuming millions of acres. In recent years, close to 10 million acres annually have been lost to wildland fires (in contrast to less than half that acreage before 2000). The intensity of these fires is sterilizing the soil and leading to extensive post-fire flooding because there is no vegetation left to check rainwater runoff. Forest conditions (including a beetle infestation that has left behind 40 million acres of dead trees) have also left them vulnerable.

Dead trees are fuel for extreme wildfires. The intensity of these fires is sterilizing the soil and leading to extensive post-fire flooding because there is no vegetation left to check rainwater runoff. Megafires have "exploded in number" over the last decade. Shorter and warmer winters followed by hotter and drier summers have significantly extended the fire season. Megafires threaten not only human life and property but wildlife habitat, water supplies and the electric grid.]

GLOBAL STUDIES LAW REVIEW: O'Connell, Mary Ellen, 21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs (March 23, 2015). 13 Global Studies Law Review, 515 (2015); Notre Dame Legal Studies Paper No. 1506. Link at: http://ssrn.com/abstract=2583992.

GREENPEACE: Hirsch H, Becker O, Schneider M, and Froggatt A, Nuclear Reactor Hazards: Ongoing Dangers of Operating Nuclear Technology in the 21st Century, Report for Greenpeace International, Apr 2005. http://www.greenpeace.org/seasia/th/PageFiles/106897/nuclearreactorhazards.pdf.

[Helmut Hirsch, PhD is founder and staff scientist of Gruppe Ökologie Hannover and a member of numerous expert commissions providing advice on nuclear and spent fuel storage safety and security issue to European groups in Germany and Austria. Dr Hirsch also participating in a study of possible hazards pertaining to dry cask storage at Skull Valley, Utah. Oda Becker, PhD, a physicist, specializes in nuclear power and spent fuel safety and has been a consultant to the government of Austria. She contributed to studies of the vulnerability of nuclear facilities to air plane crashes and terror attack. Mycle Schneider is a Paris-based nuclear power, environmental and energy planning expert who has consulted for governmental bodies of France and Belgium, the European Commission, and the International Atomic Energy Agency (IAEA). This report describes the inherent flaws of nuclear power plants. Separate chapters are devoted to assessment of risks associated with the management of spent nuclear fuel, the aging of operational plants, the terrorist threat to nuclear power and the risks associated with climate change.

Among the main conclusions: “Highly radioactive spent fuel mostly is stored employing active cooling. If this fails, this could lead to a major release of radioactivity, far more important than the 1986 Chernobyl accident”. (Executive Summary, p 5)]

INSIDE CLIMATE NEWS: stern, Marcus and Sebastian Jones, Pipeline Safety Chief Says His Regulatory Process Is ‘Kind of Dying,’ Inside Climate News, Sep 11, 2013. http://insideclimatenews.org/news/20130911/exclusive-pipeline-safety-chief-says-his-regulatory-process-kind-dying.

INSIDE CLIMATE NEWS: Douglass, Elizabeth, Exxon Knew Its Ruptured Pipeline Was Old, Defective and Brittle, and Still Added New Stresses, Inside Climate News, Aug 12, 2013. http://insideclimatenews.org/news/20130812/exxon-knew-its-ruptured-pipeline-was-old-defective-and-brittle-and-still-added-new-stresses.

INSIDE CLIMATE NEWS: Song, Lisa, Safety Compromised by Missing Rules on Oil and Gas Pipelines, GAO Says, Inside Climate News, Feb 5, 2013. http://insideclimatenews.org/news/20130205/pipeline-safety-gao-report-emergency-response-phmsa-enbridge-yellowstone-river-keystone-xl-valves.

INSTITUTE FOR POLICY STUDIES (IPS): Alvarez, Robert, Spent Nuclear Fuel Pools in the U.S.: Reducing the Deadly Risks of Storage, Report, Institute for Policy Studies (IPS), May 2011. http://www.ips-dc.org/reports/spent_nuclear_fuel_pools_in_the_us_reducing_the_deadly_risks_of_storage.

[Robert Alvarez, is a former Senior Advisor to the U.S. Secretary of Energy.

Over the past 30 years, there have been at least 66 incidents at U.S. reactors in which there was a significant loss of spent fuel water. Ten have occurred since the Sep 11 attacks. Over several decades, significant corrosion has occurred of the barriers that prevent a nuclear chain reaction in a spent fuel pool — some to the point where they can no longer be credited with preventing a nuclear chain reaction.

The NRC depends largely on the industry self-reporting problems. Strains are being placed on crowded spent fuel pools of old reactors. Systems for keeping pools cool and clean are being overtaxed, as reactors generate hotter, more radioactive, and more reactive spent rods. Increases of the level of fissionable uranium-235 to enable longer operating periods can cause the protective cladding around a spent fuel rod, to thin and become brittle. It also builds higher pressure from hydrogen and other radioactive gases within the cladding, all of which adds to the risk of failure. The cladding is less than one millimeter thick (thinner than a credit card) and is a crucial barrier to the escape of radioactive material.]

INSTITUTE FOR RESOURCE AND SECURITY STUDIES: Thompson GR, Risk-Related Impacts from Continued Operation of the Indian Point Nuclear Power Plants, Report of the Institute for Resource and Security Studies, Cambridge, MA, for Riverkeeper, NY, Nov 28, 2007. http://pbadupws.nrc.gov/docs/ML1209/ML120970089.pdf.

[Gordon Thompson, PhD, Director of the Institute for Resource and Security Studies in Cambridge, Massachusetts, is an internationally-recognized expert in the safety issues and security hazards associated with nuclear facilities. He has worked on committees advising the NRC, and was also associated with the fusion research program of the UK Atomic Energy Authority.]

INSTITUTE FOR RESOURCE AND SECURITY STUDIES (IRSS): Thompson G, Robust Storage of Spent Nuclear Fuel: A Neglected Issue of Homeland Security, Report of Institute for Resource and Security Studies for the Citizens Awareness Network, January 2003. http://www.nirs.org/reactorwatch/security/sechossrpt012003.pdf.

[Gordon Thompson, PhD, is Director of the Institute for Resource and Security Studies. In this study he reviewed the ways in which spent fuel pools are vulnerable to attack**.** Dr. Thompson concluded that a nuclear fire in the spent fuel pool of Indian Point Unit 2 would release enough cesium-137 “to render about 95,000 square kilometers of land uninhabitable" – the geographic equivalent of about 75% of New York State.]

INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA): The Fukushima Daiichi Accident, Report by the Director General International Atomic Energy Agency, Mar 2015.

INTERNATIONAL NETWORK OF ENGINEERS AND SCIENTISTS AGAINST PROLIFERATION (INESAP): Zhang, H, Radiological Terrorism: Sabotage of Spent Fuel Pools, International Network of Engineers and Scientists Against Proliferation report (2003); 22: 75-78.
http://belfercenter.hks.harvard.edu/publication/364/radiological_terrorism.html.

[This paper is authored by Hui Zhang of the Project on Managing the Atom at the the Project on Managing the Atom at the Belfer Center for Science and International Affairs, Harvard Kennedy School.

"A 400 t PWR pool holds about 10 times more long-lived radioactivity than a reactor core. A radioactive release from such a pool would cause catastrophic consequences. One major concern is the fission product cesium-137 (Cs-137), which made a major contribution (about three quarters) to the long-term radiological impact of the 1986 Chernobyl accident. A spent fuel pool would contain tens of million curies of Cs-137. Cs-137 has a 30 year half-life; it is relatively volatile and a potent land contaminant. In comparison, the April 1986 Chernobyl accident released about 2 Mega Curies (MCi) Cs-137 into the atmosphere from the core of the 1,000 MWe unit 4. It is estimated that over 100,000 residents were permanently evacuated because of contamination by Cs-137.The total area of the radiation-control zone is about 10,000 km², in which the contamination level is greater than 15 Ci/km² of Cs-137."

"Assuming a 50-100% Cs137 release during a spent fuel fire, the consequence of the Cs-137 exceed those of the Chernobyl accident 8-17 times (2MCi release from Chernobyl). Based on the wedge model, the contaminated land areas can be estimated. For example, for a scenario of a 50% Cs-137 release from a 400 t SNF pool, about 95,000 km² (as far as 1,350 km) would be contaminated above 15 Ci/km² (as compared to 10,000 km² contaminated area above 15 Ci/km² at Chernobyl)."

The greatest concern is the possibility of significant release of radioactivity in a spent fuel fire, especially in the case of densely packed pools. "The most serious risk is the loss of pool water, which could expose spent fuel to the air, thus leading to an exothermal reaction of the zirconium cladding, which would catch fire at about 900 °C. Thus, the Cs-137 in the rods could be dispersed into the surrounding atmosphere. Based on a *Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plant* in 2000, the US Nuclear Regulatory Commission (NRC) conceded that 'the possibility of a zirconium fire cannot be dismissed even many years after a final reactor shutdown.'"]

JAPAN DIET: Diet Report on Fukushima, 2012:
http://www.nirs.org/fukushima/naiic_report.pdf, Jun 2012.
http://warp.da.ndl.go.jp/info:ndljp/pid/3856371/naiic.go.jp/en/report/.

[In late 2011 Japan enacted the Fukushima Nuclear Accident Independent Investigation Commission (NAIIC Act) and the Diet (one of the three branches of the Japanese government) established a Commission independent of the parties involved in the accident, with powerful investigative authority, including the legal power to demand documents and obtain testimony. The report is sometimes called the "NAIIC Report, but is most commonly referred to as the "Diet Report." The Diet Commission investigation included more than 900 hours of hearings, interviews of 1,167 people, and 3 town hall meetings to hear firsthand the experiences of evacuees.]

JOURNAL NEWS: Tumulty, Brian, County not told of cyber attack, Journal News, Dec 23, 2015. http://www.lohud.com/story/news/2015/12/22/cyber-attack-rye-dam-raises-concerns/77755474/.

[A December 21, 2015, Wall Street Journal report revealed that Iranians had launched a cyber attack on a dam in Westchester County, NY in 2013. Westchester County is part of the New York City-area Joint Terrorism Task Force, which consists of federal, state and local law enforcement agencies. Westchester County officials said they were never told about the cyber attack on the dam by their task force partners. The attack involved a hack on controls – a cellular modem – of the Bowman Avenue Dam owned by the city of Rye Brook. Officials said the hacking incident raises concerns about the vulnerability of other infrastructure. "'When we look at other potential targets such as Indian Point or a natural gas pipeline running near Indian Point — like the proposed Spectra Algonquin Pipeline — it's clear that we must do more to assess and address potential vulnerabilities to a cyber attack,' Rep. Eliot Engel, D-the Bronx, said." Sen. Chuck Schumer, D-N.Y., is calling on the DHS to investigate the vulnerability of critical infrastructure.]

Koppel, Ted, "Light's Out," Crown Publishers, 2015.

[Ted Koppel, former anchor and managing editor of ABC's "Nightline," and a premier investigative reporter, presents the case in this book that a major cyberattack on America's power grid is entirely feasible and potentially catastrophic. A well-designed assault on one of the nation's three electric power grids could cripple infrastructure on a vast scale and the federal government has no plan for the aftermath of a long power outage.

CENTCOM Commander General Lloyd Austin tells Koppel, "'It's not a question of if, it's a question of when.'"]

MORELAND COMMISSION: Moreland Commission On Utility Storm Preparation and Response, Final Report, Jun 22, 2013. http://www.governor.ny.gov/assets/documents/MACfinalreportjune22.pdf.

NATIONAL RESEARCH COUNCIL: Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report, National Research Council Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage, Board on Radioactive Waste Management,

National Academies Press, Washington DC (2006) (*public version of classified 2004 report*). **http://www.nap.edu/catalog.php?record_id=11263.**

NBC: Roberts, Chris, PG&E Substation Attack Was "Significant" Act of Terrorism, Official Tells Wall Street Journal, NBC News, Feb 6, 2014. http://www.nbcbayarea.com/news/local/Terrorist-Attack--San-Jose-Pacific-Gas-Electric-Substation-243731551.html.

[In the dead of night on April 16, 2013, a Thursday, someone with knowledge of how a major electrical substation works snuck into the sensitive area at the Pacific Gas & Electric Company's Metcalf power substation southeast of San Jose, California. He (or she) cut fiber cables to knock out 911 and cell phone service. Then, he and/or an accomplice took more than 100 shots from a high-powered rifle to "methodically" make transformers overheat and shut down, knocking out the substation. The attacker(s) then escaped.

Mark Johnson, a former PG&E official told the Wall Street Journal, "'My personal view is that this was a dress rehearsal.'" Jon Wellinghoff, Chairman of the Federal Energy Regulatory Commission at the time of the attack, called it "'the most significant incident of domestic terrorism involving the grid that has ever occurred'" in the US.]

NEWSWEEK (EUROPE): Phillips, Catherine and Conor Gaffey, Most French Nuclear Plants 'Should Be Shut Down' Over Drone Threat, Europe Newsweek, Feb 24, 2015. http://europe.newsweek.com/most-french-nuclear-plants-should-be-shut-down-over-drone-threat-309019.

[In 2014, unmanned drones were spotted flying over at least 13 nuclear power stations in France. On January 3, 2015, two drones were spotted flying over a nuclear facility in Nogent-sur-Seine, France. Greenpeace became aware of another flyover sighting on January 28, 2015. A French government blackout blocked further reports.

John Large, a nuclear security expert at consulting engineers Large & Associates (London), was commissioned by Greenpeace France to evaluate and report on the spate of flyovers. He concluded that readily-available commercial drones carrying small payloads of explosives could initiate a nuclear plant disaster. He told Newsweek: "'You don't need massive amounts of force to allow a nuclear plant to go into instability. The plant has enough energy to destroy itself. Drones can be used to tickle the plant into instability.'"

In a coordinated attack, one drone could be directed to hit the distribution grid serving the plant, depriving the facility of off-site power. Other drones could then target the backup diesel generators.

Lange says the risks of nuclear power need reassessment in light of the aging of many reactors and the increased danger of terrorists targeting them with modern and readily available hardware such as unmanned drones. "'If the risk of a nuclear plant's design, age and location is unacceptable, governments must consider closing those plants down,' he says."

Large's confidential report into the flyovers found that drones would be capable of avoiding nuclear plant defenses, which were not designed to protect against with agile, airborne technology. Caroline Baylon, a cyber security expert at Chatham House, who has researched the drone threat, agrees: "'The French flyovers highlighted the fact that nuclear power plants have not been designed to defend against drones. Because drones are so small, conventional radar cannot detect them. There's a huge vulnerability there.'"]

NEW YORK DEPARTMENT OF STATE: Perales, Cesar A, New York Secretary of State, Department of State, Letter to Fred Dacimo, Vice President Operations License Renewal, Entergy Nuclear Northeast Indian Point re: F-2012-1028, Coastal Zone Management Act Consistency Determination, Indian Point Nuclear Generating Unit Nos. 2 & 3, NRC License Nos. DPR-26 and DPR-64, NRC Docket Nos. 50-247 and 50-286, Nov 6, 2015. http://www.riverkeeper.org/wp-content/uploads/2015/11/Indian-Point-Consistency-Decision-11062015.pdf.

[Notification of New York Department of State determination not to grant Entergy's request for a Coastal Consistency Determination for Indian Point due to numerous concerns about Indian Point, including:

Indian Point is in the nation's most heavily populated region. The site is about 24 miles north of New York City. Some 17 million people live within 50 miles of the facility. No other nuclear reactors in the US comes close to Indian Point in terms of surrounding population. (The NRC has noted most reactor sites in the US have population densities of less than 200 persons per square mile. Indian Point has over 2,000 persons per square mile.)

An accident has the potential to "destabilize the real estate market, infrastructure, and the economy in New York City and surrounding municipalities." (p 2)

The plant's history of operational accidents including transformer explosions and other component malfunctions.

Indian Point Units 2 and 3 are in the highest category of seismic hazard in the nation relative to the original plant seismic design basis as well as ground motion. Indian Point sits extremely close to the intersection of two active seismic faults. A 2008 Columbia University seismology concluded: "'Indian Point is situated at the intersection of the two most striking linear features marking the seismicity and also in the midst of a large population that is at risk in case of an accident to the plants. This is clearly one of the least favorable sites in our study area from an earthquake hazard and risk perspective.'" (p 12) In addition, the NRC has reported Unit 3 has the highest risk of serious damage to its nuclear core in the event of earthquake.

"On May 13, 2011, the NRC issued seismic vulnerability inspection reports of Indian Point Unit 2 and unit 3. The inspection reports were written 'to capture the need to evaluate the beyond design basis aspect of simultaneous 8.5.b events on both units.' These '8.5.b events' are simultaneous external natural events and consequences beyond the original plant design basis, such as large fires, explosions on site or flooding conditions on site which test the licensee's capability to mitigate station blackout (SBO) conditions and identify the potential that the equipment's function could be lost during seismic events possible for the site. The NRC Staff reported that Entergy identified a number of potential vulnerabilities at Units 2 and 3 regarding firefighting following a safe shutdown earthquake (SSE). The potential vulnerabilities stem from

the fact that the fire protection system in non-safety related buildings, buries/underground fire headers, fire pumps, and the city water makeup supply are not seismically designed which could result in a loss of portions of the fire protection system following a SSE." The NRC inspectors also identified other events beyond design and licensing basis that could pose a challenge, to witt: "'1. Generally, reactor sites were not required and did not implement mitigating actions to cope with an SBO[station blackout conditions resulting from a loss of all alternating current power] in conjunction with a seismic event; and 2. During beyond design basis events, in which the SAMGs [Severe Accident Management Guidelines] direct depressurizing the PWR containment, conditions could exist in which mitigation equipment is damaged due to elevated containment pressures and potentially prevent containment depressurization and/or isolation.'" (p 11)

For over 40 years the Indian Point nuclear facilities have been damaging the coastal resources of the Hudson River estuary. Radioactive leaks from Indian Point's systems – including two different spent fuel pools – have resulted in large plumes of groundwater contamination under the site and radioactive leaks from Indian Point's Unit 2 spent fuel pools have already reached the Hudson River.

Indian Point is 6 miles west of the New Croton Reservoir in Westchester County which is part of the New York City reservoir system and provides drinking water to 9 million people in New York City. New York City contemplates using water directly from the Hudson River as a backup water supply. The communities of Poughkeepsie, Wappingers Falls, Highland, Port Ewen, the Village of Rhinebeck, East Fishkill and parts of Hyde Park use the river for drinking water. Future leaks to the groundwater or airborne radiological releases risk contaminating drinking water.

"An accidental release of radiation from the facilities could contaminate drinking water supplies and render uninhabitable large swaths of property in the NYC Metropolitan region. Such a catastrophe would cause dramatic human as well as economic losses. Replacing radionuclide-contaminated drinking water resources for millions of City residents would likely be at unimaginable expense." (p 28) "Additional radiological releases could destabilize the real estate, infrastructure, and the economy in New York City and other regional municipalities." (p 30)

Indian Point was constructed close to the river bank and sits at a relatively low point in the Hudson River valley. The shoreline is at risk of flooding during extreme storm events resulting to possible shutdown of cooling water intake pumps, loss of electrical power and dispersal of contaminants into floodwaters that drain into the river. Projected future flood maps show that the water intake structures, pier, and low lying structures may flood during extreme flood events. Grade elevation at the site is approximately 15 feet. "Storm surges and sea level rise as a result of climate change are also major contributors to flooding threats and risk within the Hudson River estuary." (p 14)

Just two high powered transmission lines physically connect Indian Point to the electrical transmission grid. These are linked to the Buchanan electrical substation across the road near the entrance to the Indian Point facility. The final 100 feet of the lines are offsite and cross over a public road (Broadway) to enter a Con Edison substation. The Buchanan substation and the regional transmission system were designed and constructed before Indian Point was sited. Vulnerability to storms was illustrated when Sandy forced a scram of Unit 3 in response to electrical grid disturbances.

"[E]lectromagnetic interference can occur between electrical power lines and adjacent gas pipelines in shared right-of-ways with potentially disastrous consequences." (p 15) Overhead

power lines may induce voltages on the metallic pipelines running in close vicinity leading to serious adverse effects, especially corrosion effect on metal pipelines.

The spent fuel pools at Indian Point store far more radioactive material than inside the active nuclear reactors but have no containment structure. Entergy's practice involves packing the existing spent fuel pools to their maximum capacity. When the pools were designed and constructed decades ago, the pools were deemed "'temporary'." (p18) Two of the pools on site have leaked radiation into the environment. The original licenses in 1973 (for unit 2) and 1975 (for unit 3) authorized the pools to each hold 241 spent fuel assemblies. Since then the NRC has allowed Indian Point to hold 5 times the original limit. As of 2015, approximately 1,500 tons of spent nuclear fuel is stored in Indian Point's densely packed spent fuel pools.

Some of the older nuclear waste has been transferred from the spent fuel pools into dry cask storage on site. "The dry casks are placed on an open air concrete pad with no protective barriers or containment structures. … The NRC has raised concerns about dry cask storage design flaws with the cask model currently being used at Indian Point and about the cask manufacturer's inadequate quality assurance program. In the event of a design and/or manufacturing flaw that results in even a hairline fracture in the steel casing and/or concrete casing of the dry cask, an undetermined amount of radiation may leak from the storage units. There is as of yet no safe mitigation procedure to transfer the nuclear waste from a faulty dry cask storage unit to a new safe dry cask storage unit, and there would be no room to place the spent nuclear fuel waste back into the spent fuel pools for temporary safe storage." (p 36)

"During its 40 years of operation, Indian Point has had many incidents, reactor scrams, operational errors and equipment malfunctions. … As Indian Point ages and components degrade, additional events may occur. Given to its history of equipment problems, its proximity to the world's financial center and the severe consequences of a major accident on public health, the environment and the economy, Indian Point is a nuclear facility that remains a coastal concern." (pp 19-20, {*pages list some of the emergency shutdowns and radioactive leak events}*)]

NEW YORK TIMES: Perlroth, Nicole, Infrastructure Armageddon, New York Times, Oct 15, 2015. http://bits.blogs.nytimes.com/2015/10/14/online-attacks-on-infrastructure-are-increasing-at-a-worrying-pace/.

The Department of Homeland Security announced in 2014, that it was investigating an attack against 1,000 energy companies across Europe and North America. According to Dell Security, the number of attacks against industrial control systems more than doubled from 163,228 in January 2013 to 675,186 in January 2014 – with most attacks occurring in the US, UK and Finland.

In 2012, former Defense Secretary Leon E. Panetta warned that hackers with malicious intent derail trains loaded with passengers or lethal chemicals: "They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country."

In 2012, 23 gas pipeline companies were hacked by online spies, according to a Homeland Security report. Private investigators later linked the attack to China.

In a 2012 attack against Telvent, an information technology and industrial automation company later acquired by Schneider Electric, Chinese hackers made off with its product source code and blueprints to facilities operated by its customers, which include 60% of the pipeline operators in North America.

In 2012, as well, Saudi Aramco, the world's largest oil company, was attacked. Data on workers' hard drives was replaced by the image of a burning American flag. US intelligence officials attributed the sabotage to hackers in Iran. Secretary Panetta called the Aramco sabotage "a significant escalation of the cyberthreat." Two weeks later, a similar attack was launched against the Qatari oil giant RasGas.

In the Aramco and RasGas attacks, hackers penetrated corporate networks and forced servers offline, but failed to gain control over industrial production systems.

However, in 2014, a German federal agency disclosed that hackers attacking a steel mill were able to cross from the company's corporate network to its production systems, causing significant damage to a blast furnace.

In early October 2015, in a test of utility defenses, a group from the Washington State National Guard were able to break into the state's Snohomish County Public Utility District computer system via an email in under 22 minutes.

Joe Weiss, founder of the consultancy Applied Control Solutions, said the success of the Washington utility hack was not surprising. Weiss manages a database of 750 incidents that affected control systems and is most disturbed that most were not classified as attacks at all. "'What that tells you is that not only do we not have the mitigation, we don't even have any type of adequate forensics to know this is happening, and whether it was intentional or unintentional,' he said."

In many cases – like a computer outage that took down computers at Kennedy International Airport in New York, Logan Airport in Boston, and other airports across the country late in the day on October 14, 2015, a Wednesday – the problem is never tied to hacks. The Department of Homeland Security tweeted that the airport computer problems were due to a "'brief outage that lasted 90 minutes'" on the US Customs and Border Protection's computer processing systems.

"But Mr. Weiss said in most cases, forensics investigations were still not adequate enough to nail down the real source of such incidents. He said the same was true across the electric, water, oil, gas, and nuclear industries.

'It's not like with weapons, where you know where it's coming from,' Mr. Weiss said. "With cyber- and control systems, you don't necessarily know.'"]

NEW YORK TIMES: Wald, Matthew L., Ex-Regulator Says Reactors Are Flawed, New York Times, Apr 8, 2013. http://www.nytimes.com/2013/04/09/us/ex-regulator-says-nuclear-reactors-in-united-states-are-flawed.html .

[All nuclear power reactors now in operation in the United States have a safety problem that cannot be fixed Gregory B. Jaczko, former Chairman of the NRC Chairman told an audience at the Carnegie International Nuclear Policy Conference in Washington.
Asked why he did not make these points when he was chairman, Dr. Jaczko said in an interview after his remarks:
"'I didn't really come to it until recently.
"'I was just thinking about the issues more, and watching as the industry and the regulators and the whole nuclear safety community continues to try to figure out how to address these very, very difficult problems,' which were made more evident by the 2011 Fukushima nuclear accident in Japan, he said. 'Continuing to put Band-Aid on Band-Aid is not going to fix the problem.'"]

NEW YORK TIMES: Wald, Matthew L, and John Schwartz, Weather Extremes Leave Parts of the U.S. Grid Buckling, New York Times, Jul 26, 2012. http://www.nytimes.com/2012/07/26/us/rise-in-weather-extremes-threatens-infrastructure.html.

[Leading climate models indicate that weather-sensitive parts of the infrastructure will confront increasing extreme weather episodes along with shifts in weather patterns to both hot and cold.

Vicki Arroyo, head of the Georgetown Climate Center at Georgetown University Law Center in D.C., a clearinghouse on climate-change adaptation strategies, said, in general, nobody in charge of anything made of steel and concrete can plan based on past trends.

Tom Scullion, senior research engineer at the Texas Transportation Institute at Texas A&M University, noted highways have been designed with traditional climate, temperature and rainfall conditions. "'When you get outside of those things, man, all bets are off.' As weather patterns shift, he said, 'we could have some very dramatic failures of highway systems.'"

The stresses were evident during the July 2012 heat wave that hit the US. "From highways in Texas to nuclear power plants in Illinois, the concrete, steel and sophisticated engineering that undergird the nation's infrastructure are being taxed to worrisome degrees by heat, drought and vicious storms." On a single day in July 2012, a US Airways regional jet became stuck in asphalt that had softened in 100°F temperatures, and a subway train derailed after the heat stretched the track so far that it kinked, creating a sharp angle into a stretch that was supposed to be straight. Scullion said, in parts of Texas, heat and drought shrink clay-rich soils under highways leading to "'horrendous cracking'" and in Northeastern and Midwestern states the heat caused highway sections to expand beyond their design limits, press against each other, and "'pop up,'" creating potentially dangerous bumps.

Storms and excessive warmth and dryness threaten the grid as well. "'We've got the 'storm of the century' every year now,'" said Bill Gausman, a Senior VP at the Potomac Electric Power Company, which took 8 days to recover from a June 29, 2012 "derecho" storm that raced from the Midwest to the Eastern Seaboard, knocking out power for 4.3 million people in 10 states and the District of Columbia. In July 2012, a twin-unit nuclear plant in the Chicago area had to operate pulling in water for cooling that was as high as 102°F. The Midwest Independent System Operator reported another power plant had had to shut because the body of water from which it draws its cooling water had dropped so low that the intake pipe became high and dry. Still another plant had to cut back generation because of too warm cooling water.]

NORTH AMERICAN ELECTRICAL RELIABILITY CORPORATION and ENERGY DEPARTMENT: High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, Joint Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop, Jun 2010. http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf.

NUCLEAR INFORMATION AND RESOURCE SERVICE (NIRS): Damveld H and Bannick D, Management of Spent Fuel and Radioactive Waste: State of affairs – A worldwide overview, NIRS Nuclear Monitor, 746/7/8, May 2, 2012. http://www.nirs.org/mononline/nm746_48.pdf.

NUCLEAR INTELLIGENCE WEEKLY: Former NRC Chairman Calls for Nuclear Phaseout in US, Says Plants Aren't Safe, Nuclear Intelligence Weekly (2013); 7 (13): 3-4. http://www.beyondnuclear.org/storage/mark-1-campaign/fof/jaczko_ni1303293.pdf.

[Former NRC Chairman Gregory Jaczko says that the current fleet of operating plants in the US should be phased out because regulators cannot guarantee against an accident causing widespread land contamination. Jaczko said the commissioners were "'just rolling the dice'" in dealing with severe accidents. He is not alone among former NRC commissioners and other officials.

"'The next accident is going to be something that no one predicted. At a certain point you have to review the fundamental problem." The low probability high consequences risk analysis is not a fair trade, Jaczko said, adding that aging US reactors should not operate past their 40-year lifetimes.]

OAK RIDGE NATIONAL LABORATORY: Wang J-AJ, Wang H, Jiang H, Bevard BB, Howard RL, and Scaglione JM, High Burn-Up Spent Nuclear Fuel Vibration Integrity Study 15134, Oak Ridge National Laboratory (ORNL) and High Temperature Materials Laboratory (HTML)Technical Report ORNL/TM-2014/214 (May 1, 2015), SciTech Connect Abstract. http://www.osti.gov/scitech/biblio/1210132.

[A new cyclic Integrated Reversible-bending Fatigue Tester (CIRFT) method has been designed by Oak Ridge National Lab to successfully demonstrate the controllable fatigue fracture on high burnup (HBU) spent nuclear fuel (SNF) under normal vibration mode conditions.

Because of the "inhomogeneous composite structure of the SNF system, the detailed mechanisms of the pellet-pellet and pellet-clad interactions and the stress concentration effects at the pellet-pellet interface cannot be readily obtained from a CIRFT system measurement."

Finite element analyses (FEAs) are thus used to translate the global moment-curvature measurement into local stress-strain profiles for further investigation.

The major findings of the lab's cyclic Integrated Reversible-bending Fatigue Tester (CIRFT) investigation into fatigue fracture of high burnup spent fuel under normal vibration mode conditions shows spent nuclear fuel (SNF) system interface bonding plays an important role in fuel vibration performance. Fuel structure contributes to spent nuclear fuel system stiffness and, there are "significant variations in stress and curvature of SNF systems during vibration cycles resulting from segment pellets and clad interactions. SNF failure initiates at the pellet-pellet interface region and appears to be spontaneous."]

PACIFIC GAS AND ELECTRIC COMPANY (PG&E): FG&E Fire Response and Resources, accessed Sep 20, 2015. http://www.pge.com/en/safety/naturaldisaster/wildfire/resources.page?WT.ac=MyHome_Landing_WildfireResources.

[The California utility PG&E reports its mid-September damage assessment "revealed significant impacts to PG&E's electrical assets" caused by the Butte and Valley fires. "The fire has damaged power lines and poles, causing outages in the area, and it continues to threaten PG&E equipment and facilities."

{*As of September 20*} PG&E has identified 892 transmission and distribution pole locations that require repair, there are additionally areas where cross arms and other equipment will need to be replaced. PG&E workers have already replaced more than 250 damaged transformers.

"It can take a {*sic*} multiple crews and several hours to set one utility pole. It is a difficult job working in hazardous conditions… Once crews access a work site, they must evaluate the damaged pole which is likely to be unstable, and safely remove it. Heavy equipment is used to drag new poles uphill, crews dig a hole, set the pole and string conductor, while standing in a foot of ash and breathing ash and dust." In many of the work locations, fire impacts have made the ground unstable creating hazardous conditions for the workers.

The company has also brought in 1,300 employees to help mitigate the risks including enhanced ground patrols to inspect, and prune or remove dead or dying trees that could fall into lines and spark fire.]

Perkins, Richard H, Letter to Hubert T. Bell, Office of the Inspector General of the NRC, Sep 14, 2012. http://big.assets.huffingtonpost.com/igletter.pdf.

[Richard L. Perkins, an engineer with the NRC Division of Risk Management, writes:

"[T]he Nuclear Regulatory Commission (NRC) has intentionally mischaracterized relevant and noteworthy safety information as sensitive, security information in an effort to conceal the information from the public. This action occurred in anticipation of, in preparation for, and as part of the NRC's response to a Freedom of Information Act request for information concerning the *generic* issue investigation on *Flooding of U.S. Nuclear Power Plants Following Upstream Dam Failure*. Specifically requested was the completed screening analysis report for this issue, of which I am the lead author. Portions of the publically released version of this report are redacted citing security sensitivities, however, the redacted information is of a general descriptive nature

or is strictly relevant to the safety of U.S. nuclear power plants, plant personnel, and members of the public. The Nuclear Regulatory Commission staff has engaged in an effort to mischaracterize the information as security sensitive in order to justify withholding it from public release using certain exemptions... The Nuclear Regulatory Commission staff may be motivated to prevent the disclosure of this safety information to the public because it will embarrass the agency. The redacted information includes discussion of, and excerpts from, NRC official agency records that show the NRC has been in possession of relevant, notable, and derogatory safety information for an extended period but failed to properly act on it. Concurrently, the NRC concealed the information from the public."]

PROCEEDINGS OT THE NATIONAL ACADEMY OF SCIENCES: Brummitt CD, Hines PDH, Dobson I, Moore C, and Souza RMD, Transdisciplinary electric power grid science (with Supporting Information) Proceedings of the National Academy of Sciences (PNAS) (2013); 110 (30): 12159. http://arxiv.org/pdf/1307.7305.pdf.

[Paper by scientists from the Departments of Mathematics, Mechanical and Aerospace Engineering, and Computer Science, and the Complexity Sciences Center at the University of California, Davis; the School of Engineering at the University of Vermont, ECpE Department, Iowa State University, Ames, and the Santa Fe Institute, describes the need to produce new risk models for power grids and infrastructure. The focus is on cascading failures, such as the blackout which affected Northeastern North America in 2003 and widespread grid failures triggered by Superstorm Sandy. Such events involve detailed feedbacks of multiple systems. The complexity of web interacts resembles an ecosystem.

The authors note: "Power grids comprise more than physical infrastructure…they are also social and market systems, and challenges span all three of the physical, human and market layers. At the center lies what engineers understand best: the electrical infrastructure. Next, information and communication systems monitor and control the electrical infrastructure at increasing levels of detail using new technology. Novel capabilities … risk introducing privacy concerns, security vulnerabilities, and dependence between electricity and information infrastructure."

Modeling must incorporate the feedback loops between climate change, power systems, infrastructure, and human behavior. Examples of the many complicated mechanisms involved, for example in blackouts, include thermal overloads, relay failure, voltage collapse, dynamic instability and operator error. Risk spreads also among infrastructures, such as via computer viruses.

"The National Academy of Sciences report on robustness and resilience of the electric power system in the United States highlights dangers from the power system's age, inadequate guards against malicious attack, and interdependence with other infrastructure (like wireless communication), all of which exacerbate risks…caused by extreme weather or by terrorist attack." The risks include blackouts lasting months because of damage to hard-to-replace transformers.

Current state-of-the-art models capture only a subset of failure mechanisms. Tackling problems with large-scale feedbacks among different systems requires a incorporation of transdisciplinary knowledge, which may be called "multiple disciplinary."]

PUBLIC EMPLOYEES FOR ENVIRONMENTAL RESPONSIBILITY (PEER): Flood Risk to Reactors Underestimated and Unaddressed, Public Employees for Environmental Responsibility Press Release, Sep 23, 2013. http://www.peer.org/news/news-releases/2013/09/23/flood-risk-to-reactors-underestimated-and-unaddressed/.

[Upstream dam failures may cause Fukushima-level disasters at multiple nuclear plants. The NRC does not consider the combination of dam failure and extreme weather events such as wind-generated waves and runup.]

Rauhut, Kathryn and Debra Decker, New York Times letter, Jan 25, 2016. http://www.nytimes.com/2016/01/25/opinion/nuclear-cybersecurity-why-we-should-worry.html.

[Authors are with the Stimson Center's Managing Across Boundaries Initiative. Ms. Rauhut is a nonresident fellow in Vienna, and Ms. Decker is a senior adviser.

The lack of cybersecurity regulations in the nuclear industry is, in fact, a small piece of a larger problem. "There are no internationally binding standards or related regulations at all in nuclear security. Cyber is the tip of an iceberg that is melting fast."

"Nuclear facilities are exposed to risks — from hackers to ISIS — that were not in our lexicon when many facilities were built. This lack of understanding of new and emerging threats and corresponding underspending in security are pervasive."]

Resnikoff, Marvin, and Donna Gilmore, High Burnup Nuclear Fuel – Pushing the Safety Envelope, High burnup fuel Fact Sheet, Jan 2014. http://sanonofresafety.org/2014/01/08/high-burnup-fuel-fact-sheet-2/. See also fact sheet: http://www.nwtrb.gov/meetings/2013/nov/resnikoff_burnup.pdf.

[Marvin Resnikoff, a nuclear physicist and expert on radioactive waste. High burnup fuel is fuel which has burned in the reactor for more than 45 Gigawatt days per Metric Ton of Uranium (GWd/MTU). High burnup is cheaper for nuclear operators to use than conventional fuel and the NRC has allowed its use in US reactors since the late 1990s. "Because of the poor economics of nuclear power, utilites are pushing the limits for how long fuel remains in reactors with dire consequences." (p 2) As of 2012, most fuel in pools for future loading is high burnup.

High burnup fuel is dangerously unpredictable and unstable in storage – even in the short-term. HBU requires more storage space between fuel assemblies due to higher heat, radioactivity and instability. The Department of Energy has noted that burnup rates as low as 30 GWd/MTU can present performance issues including cladding embrittlement under normal and accident conditions. Many pressurized water reactors have fuel with projected burnup greater than 60 GWd/MTU.

High burnup fuel (or HBU or HBF) is over twice as radioactive and over twice as hot as traditional nuclear fuel. The higher the burnup rate and the higher the uranium enrichment, the more radioactive, hotter and unstable HBU becomes. HBU has over twice the radioactive cesium inventory of traditional fuel.

While lower burnup fuel may be removed from spent fuel pools for storage in safer dry casks after 5 years, HBU fuel requires a minimum of 7 to 20+ years of cooling in spent fuel pools. HBU has major implications for pool storage, and the current high spent fuel pool densities present an even greater risk due to inclusion of HBU. Since the cladding of HBU is brittle, there are serious unanswered questions about long duration, high temperature fires and the effect on fuel cladding.

Malevolent events are of particular concern and have not been seriously examined. “This is of particular concern with HBF, with large Cesium inventories and suspect fuel cladding.” (p 4)]

SAPE: Nuclear Regulatory Commission Withheld and Misrepresented Critical Information Used to Evaluate and Approve the Siting of the Spectra AIM Pipeline Alongside Indian Point, SAPE Press Release, Jul 15, 2016 with web link to videocast special presentation Paul Blanch to Nuclear Regulatory Commission Petition Review Board, Hendrick Hudson Library, Montrose, NY, Jul 15, 2015. http://sape2016.org/2015/07/16/nuclear-regulatory-commission-withheld-and-misrepresented-critical-information-used-to-evaluate-and-approve-the-siting-of-the-spectra-aim-pipeline-alongside-indian-point/.

[On March 3, 2015, the Federal Energy Regulatory Commission (FERC) issued a Certificate for the Spectra Energy Algonquin Incremental Market Project pipeline (AIM pipeline), a 42-inch high-pressure gas pipeline planned to be situated next to Indian Point nuclear power facility, which caught fire May 9, 2015.

A NRC email released in response to a FOIA request, revealed that a rupture of a gas pipeline of the AIM size would release gas at the rate of 376,000 kg per minute, which is nearly 1 million pounds per minute of explosive gas. Natural gas contains 10 times the energy per pound of TNT. Such a rupture could cause a blast of 4 kilotons of energy a minute. (The nuclear blasts at Hiroshima and Nagasaki were about 15 kilotons.)

A rupture of the AIM pipeline could cause continuous explosions which could destroy systems needed to shut down the Indian Point reactors, according to Paul Blanch, a nuclear engineer with 45 years of experience, who helped design nuclear plants, was formerly a consultant to Indian Point, who served as a Nuclear Navy Submarine Reactor operator and instructor.

In a statement Blanch said: “The NRC has threatened the safety of more than 20 million residents and the infrastructure of the greater NY metropolitan area and is risking trillions of dollars of damage and possibly the US economy by basing its safety assessment on a calculation that was recently obtained from the NRC under FOIA. This new information confirms that this NRC ‘calculation’ which was partially handwritten, unapproved, undated and unsigned, used fictitious, false and unsupported assumptions. This NRC calculation supported the FERC approval of the AIM project and the transportation of thousands of tons of TNT equivalent across and in the vicinity of the Indian Point nuclear plants. This ‘back of the envelope-type calculation,’ which misled Congressional representatives, FERC and the general public, must be

invalidated and an independent, transparent, structured risk assessment, as outlined in an Occupational Safety & Health Administration (OSHA) methodology, must be undertaken."]

SCIENCE AND GLOBAL SECURITY: Alvarez R, Beyea J, Janberg K, Kang J, Lyman E, Macfarlane A, Thompson G, and von Hippel FN, Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States, Science and Global Security (2003); 11 (1): 1-51. http://www.tandfonline.com/doi/abs/10.1080/08929880309006.

[This study was conducted by an eight institution team led by the physicist Dr. Frank Von Hippel, Director of the Program on Science and Global Security at Princeton University. The group included including Dr. Alison McFarlane of the Securities Studies Program at M.I.T. (prior to her appointment as NRC Chairman) and Robert Alvarez, former Senior Advisor to the U.S. Secretary of Energy.

The study discusses the risks and consequences of spent fuel pool fires. It states that a successful terrorist attack on the spent fuel storage pool at Indian Point could have consequences "significantly worse than Chernobyl." Specifically, the study determined that a catastrophic spent fuel fire could release a radiation plume that could contaminate 8 to 70 times more land than the area affected by Chernobyl.]

STRATEGIC INSIGHTS: Kesler, Brent, Cyber Attacks Against Nuclear Facilities, Edition on Cyber Security in International Relations, Strategic Insights (2011); 10 (1) 15-25. http://www.dtic.mil/dtic/tr/fulltext/u2/a541955.pdf.

UNION OF CONCERNED SCIENTISTS: Flood Risk at Nuclear Plants, Union of Concerned Scientists, web page *accessed Nov 28, 2012.* http://www.ucsusa.org/nuclear_power/making-nuclear-power-safer/preventing-nuclear-accidents/flood-risk-at-nuclear-power-plants.html.

[Flooding is a risk to safe operation of nuclear plants because flooding can damage equipment, knock out electrical systems, and disable cooling mechanisms. This is what happened at Fukushima as a result of the tsunami flooding. Natural weather events that can lead to flooding include heavy rain or snows that can cause rivers to overflow, and nor'easters and tropical storms can cause storm surges that threaten coastal plants.

"Floods from such natural weather events have caused problems at several U.S. nuclear power plants in recent years. In June 2011, unusually high water on the Missouri River, caused by a combination of heavy spring rains and Rocky Mountain snowmelt, inundated the Fort Calhoun plant in Nebraska. And in October 2012, flooding from Hurricane Sandy caused two New Jersey nuclear plants, Salem and Oyster Creek, to shut down when high water levels threatened their water intake and circulation systems."

Nuclear plants downstream from dams also face threat. In dam failure, flooding is sudden and can be catastrophic. “Unlike river overflows or hurricanes, dam failures are likely to occur with little or no advance warning, leaving plant operators scrambling to protect their facilities before the floodwaters arrive within hours.” There have been 700 dam failures in the U.S. since 1975.

In July 2011, a report released by the NRC identified 34 nuclear plants as being at heightened risk of flood damage due to upstream dam failures; Indian Point Units 2 and 3, among the plants at risk.]

UNION OF CONCERNED SCIENTISTS: Gronlund L, Lochbaum D, and Lyman E, Nuclear Power in a warming world: Assessing the Risks, Addressing the Challenges, Report of the Union of Concerned Scientists (UCS), Dec 2007. http://www.ucsusa.org/assets/documents/nuclear_power/nuclear-power-in-a-warming-world.pdf.

[“Even in the wake of the 9/11 attacks, the NRC “continues to disregard the risk of an attack on spent fuel pools at reactor sites.” (p 32) “[N]o containment buildings protect these pools, and an accident or terrorist attack that allows the water in a densely packed pool to rapidly drain away could cause the zirconium cladding on the fuel rods to catch fire and the spent fuel to melt, resulting in a significant release of highly radioactive isotopes such as cesium-137…Adding more spent fuel to these pools only compounds this potential problem, and increases the amount of radioactive material that could be released into the environment.” (p 47)]

UNION OF CONCERNED SCIENTISTS: Lyman ES, Chernobyl on the Hudson? The Health and Economic impacts of a terrorist Attack at the Indian Point Nuclear Plant, Union of Concerned Scientists report commissioned by Riverkeeper, Inc., Sep 2004. http://www.ucsusa.org/assets/documents/nuclear_power/indianpointhealthstudy.pdf.

[Edwin Lyman, PhD, a physicist, is a Senior Staff Scientist in the Global Security program at the Union of Concerned Scientists in Washington, DC, analyses the potential consequences of a severe accident at Indian Point.

In a calculation using NRC methodology, Dr. Lyman estimates economic damages (2004 dollars) could exceed $1.1 trillion.]

UNIVERSITY OF TEXAS (NUCLEAR PROLIFERATION PREVENTION PROJECT): Kirkham L and Kuperman AJ, Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current “Design Basis Threat” Approach, Report of the Nuclear Proliferation Prevention Project, LBJ School of Public Affairs, University of Texas at Austin, Aug 15, 2013. http://blogs.utexas.edu/nppp/files/2013/08/NPPP-working-paper-1-2013-Aug-15.pdf.

[Report of the Nuclear Proliferation Prevention Project at the University of Texas, commissioned by the U.S. Department of Defense, identifies Indian Point in New York, as well as other nuclear sites in the U.S., to be vulnerable to terrorist attack that could result in reactor core damage or a spent fuel pool fire and a major radioactive release. NRC Design Basis Threat rules fail to ensure safeguards of reactors and spent fuel pools against terrorist attack of even the type and

scale as that which occurred on Sep 11, 2001. Security rules do not require defense against aircraft attack or against waterborne attack of any size. "…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 Sept. 11, 2001," the study reports. "More than a decade after the worst terrorist attack in U.S. history, operators of existing nuclear facilities are still not required to defend against the number of terrorist teams or attackers associated with 9/11, nor against airplane attacks, nor even against readily available weapons such as high-power sniper rifles."]

USA TODAY: Reilly, Steve, Records: Energy Department struck by cyber attacks, USA Today, Sep 10, 2015. (Link also to web interview of Steve Reilly by Shannon Rae Green.) http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/.

[Department of Energy (DOE) computer systems were hit 1,131 times by cyberattacks over a 48 month period from 2010 to Oct 2014 a review of federal records obtained by USA Today through the Freedom of Information Act found. Attackers successfully compromised the security of DOE computer systems 159 times. Of these, 53 were "root compromises," in which the attackers gained administrative privileges to DOE computer systems.

The National Nuclear Security Administration (NNSA), a semi-autonomous agency within the DOE responsible for managing and securing the US nuclear weapons stockpile, experienced 19 successful attacks during the 4 year period.

"Incident reports submitted by federal officials and contractors since late 2010 to the Energy Department's Joint Cybersecurity Coordination Center shows a near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs."

Scott White, Professor of Homeland Security and Security Management and Director of the Computing Security and Technology program at Drexel University, commented: "'The potential for an adversary to disrupt, shut down (power systems), or worse … is real here….It's absolutely real.'"

Information on the specific nature of the attacks was redacted from the records provided to USA Today, but numerous DOE cybersecurity vulnerabilities have been identified in recent years by the department's Office of Inspector General. Manimaran Govindarasu, a professor in the Department of Electrical and Computer Engineering at Iowa State University, said the root compromises represent instances where intruders gained "super-user" privileges. "'That means you can do anything on the computer,' he said."]

USA TODAY: Reilly, Steve, Bracing for a big power grid attack: 'One is too many' Mar 24, 2015. http://www.usatoday.com/story/news/2015/03/24/power-grid-physical-and-cyber-attacks-concern-security-experts/24892471/.

[A multi-media investigation by USA Today in collaboration with Gannett newspapers and TV stations across the country involved review of thousands of pages of government records,

federal energy data and a survey of more than 50 electric utilities. Key findings include: • Cyber or physical attacks against the nation's power infrastructure are being launched at the rate of one every four days. • Transformers and other critical equipment often sit in plain view, protected only by chain-link fencing and a few security cameras. • There have been over 300 attacks on electrical infrastructure since 2011.

Security breaches have heightened concern over the possibility that vulnerabilities in the electric system could trigger a widespread lasting outage which exhausts key backup power supplies. Some experts and officials fear the rash of smaller-scale incidents may point to broader security problems with potentially devastating consequences.

Jon Wellinghoff, former Chairman of the Federal Energy Regulatory Commission, warns the power grid is "'too susceptible to a cascading outage'" because of reliance on a small number of critical substations and other physical equipment. If multiple parts fail at the same time, there is the potential for a cascading effect. "'Those critical nodes can, in fact, be attacked in one way or another,' Wellinghoff said. 'You have a very vulnerable system that will continue to be vulnerable until we figure out a way to break it out into more distributed systems.'"

A prime example of the vulnerability of grid security occurred shortly before 1 am on April 16, 2013, when attackers made a coordinated attack on Pacific Gas & Electric's Metcalf substation in northern California. The attackers severed six underground fiber-optic lines before firing more than 100 rounds of ammunition at the substation's transformers, causing more than $15 million in damage. The attackers were never caught.

At a Senate hearing in 2014, Sue Kelly, president and CEO of the American Public Power Association testified: "Shooting at substations, unfortunately, is not uncommon ... But this incident demonstrated a level of sophistication not previously seen in our sector.'"

Between 2011 and 2014, electric utilities reported 362 physical and cyberattacks that caused outages or other power disturbances to the Department of Energy (DOE). Of those, 14 were cyberattacks. Among the incidents: In 2011, an intruder broke a door lock and gained access to a critical hydro-electric converter station in Vermont. In 2013, a gunman fired multiple shots at a gas turbine power plant along the Missouri-Kansas border. In 2013, 4 bullets fired from a highway struck a power substation outside Colorado Springs. Cause for concern also arose after a simulated cyberattack conducted by the Idaho National Laboratory in 2007 exploited a vulnerability at the facility by altering the timing of a diesel generator's circuit breakers.

At a 2013 security conference in Louisville, former energy security regulator Josh Axelrod, described a "seven bullets theory" of how a mass outage could be triggered by a physical attack targeting key pieces of equipment. The Eastern power grid is highly interconnected and relies on rolling power between different utilities. "'If you know where to disable certain transformers, you can cause enough frequency and voltage fluctuation in order to disable the grid and cause cascading outages … You can pick up a hunting rifle at your local sporting goods store … and go do what you need to do,'" he said.

Thomas Popik, president of the Foundation for Resilient Societies, a Nashua, N.H.-based advocacy group, described the security system for the energy grid as "'badly broken'."

The energy industry writes and enforces its own security guidelines and decreased the number of penalties it issued by 30% from 2013 to 2014. The North American Electrical Reliability

Corporation (NERC) along with industry funded groups like the Edison Electric Institute, have fought legislation including the Grid Reliability and Infrastructure Defense Act (GRID) Act, that would eliminate the industry's self-regulation.]

U.S. CONGRESSIONAL RESEARCH SERVICE: Werner, JD, May 24, 2012. U.S. Spent Nuclear Fuel Storage, Report of the Congressional Research Service, 7-5700; R42513, May 24, 2012. https://www.fas.org/sgp/crs/misc/R42513.pdf.

[As of Dec 2011 more than 67,000 metric tons of spent fuel in more than 174,000 assemblies is stored at 77 sites (including 4 DOE facilities) in 35 states, increasing at the rate of about 2,000 metric tons per year. About 73% (67,450 metric tons) of spent fuel continues to be in spent fuel pools, which are becoming filled to capacity. At 27 sites there is no current dry cask storage capability. (Summary.) The 5 states with the largest total amount of spent nuclear fuel measured by metric tons of heavy metal content are: Illinois; Pennsylvania; South Carolina; New York; and North Carolina. The top five states with the largest amount of spent nuclear fuel in pools are Illinois: Pennsylvania; New York; North Carolina; and Alabama. (p 24.)

"In fact, virtually every site that has ever hosted a commercial nuclear reactor is currently also a storage site for SNF." (p 17) Approximately 80% of commercial spent nuclear fuel, measured by mass, is stored east of the Mississippi River. (p 23)

"Notwithstanding the mandate in the Nuclear Waste Policy Act (NWPA) and various contracts that DOE begin accepting SNF for disposal in 1998, no disposal repository has been completed or licensed." Even if the Yucca Mountain program – terminated in 2009 – were to be resumed quickly, the time required to ship nuclear waste would require an extended period of storage, with interim storage being needed until at least 2056. The current quantity of nuclear waste in the nation (at commercial and government sites) exceeds the legal capacity of the proposed Yucca Mountain repository. (p 5)

A survey of spent fuel storage in 10 nations with significant nuclear operations found that all store substantial amounts of spent fuel in pools or dry casks. France – with 13,500 metric tons of spent fuel and 2,229 cm of vitrified high level waste as of 2007 – has not yet selected a disposal site for high level waste. Finland (with 4 nuclear reactors) is the only country where a commercial nuclear waste repository site has been selected with local government support. (p 7)

The U.S. federal government has already paid out about $1 billion in claims and faces significant and growing liability arising from contracts DOE signed in 1983 and the 1987 Nuclear Waste Policy Act whereby the government was supposed to assume nuclear waste from commercial nuclear utilities. "The future estimated costs for storage of commercial SNF are approximately $500 million per year." (pp 7-8)

The Department of Energy took possession of the spent fuel and debris from the 1979 Three Mile Island plant accident. (p 25)

"In the 1970s a relatively small amount (248.7 MTU of commercial SNF was shipped from commercial reactors, including utilities in Michigan and New York, to the West Valley site in New York, which reprocessed SNF for about six years (1966 to 1972). The resulting high-level waste and contaminated facilities remain at the site. DOE has estimated that decommissioning and

environmental remediation of the contamination at the West Valley site will continue until at least 2020, cost $3.7 billion, and require indefinite long-term stewardship thereafter." (pp 25-26)

In addition to the releases of tritium contamination from spent fuel pools and other structures to groundwater at 38 commercial nuclear sites, "tritium contamination was found in groundwater from spent fuel storage pools at DOE sites, including the Brookhaven National Laboratory in New York, Hanford in Washington State, and the Savannah River Site in South Carolina….Tritium is inherently difficult to remediate, once released, because it is simply a radioactive form of hydrogen that substitutes freely with hydrogen in water and decays at a rate of about 5% per year (12.32 year half life). (p 34)

The inherent hazards of spent nuclear fuel can result in a variety of risks. "A variety of forces or 'threats' acting on spent fuel could result in containment being breached, resulting in potential exposures and risks, generally: (1) loss of power for water supply, circulation, or cooling, which can have significant consequences for SNF in wet pool storage; (2) external threats, like hydrogen explosions from adjacent reactors, or an airplane crashing into an SNF storage facility; (3) long-term degradation of SNF through chronic corrosion of cladding (e.g., hydride corrosion); and (4) leakage of contaminated water from wet pools to groundwater." (p 30) In contrast to the U.S. "Germany explicitly requires protection against risks, including 'external events' such as an attack on SNF storage, and this has resulted in construction of hardened storage buildings for dry cask storage of SNF." (p 32)

"Another potential threat to SNF storage safety is degradation of the cladding and fuel elements." The potential for degradation of SNF cladding has been well known for decades. (p 33) "'Zirconium has a high affinity for hydrogen. Absorption of hydrogen leads to hydrogen embrittlement, which can lead to failure of the zirconium tubing used as cladding for nuclear fuel. In addition, zirconium also reacts with oxygen, which can lead to corrosion.'" (p 33, fn 142, quoting Kok, Kenneth D, *Nuclear Engineering Handbook*, CRC press, 2009, at p 287)]

U.S. CONGRESSIONAL RESEARCH SERVICE: Holt, Mark, Nuclear Energy: Overview of Congressional Issues, Congressional Research Service report, Dec 23, 2015.

[When America's existing fleet of nuclear reactors were built, it was expected the spent fuel would be taken away, however, for economic and nonproliferation reasons, central waste storage and disposal facilities have proven difficult to site. "As a result, the vast majority of U.S. commercial spent fuel remains at the nuclear plantes where it was generated-totalling 71,775 metric tons in 2013 and rising at the rate of about 2,000 metric tons per year." (p 5) ' si nuclear renGiven the extensive delays in determining what to do with the nation's high level nuclear waste longer on-site storage is almost a certainty under any option. Any of the options would also face intense controversy, especially among states and regions that might be potential hosts for future waste facilities.

The nuclear industry has frequently contended that costly safety proposals are unnecessary. (p 30)]

U.S. CONGRESSIONAL RESEARCH SERVICE (CRS): Parfomak PW, Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations, U.S. Congressional

Research Service report for Congress, 7-5700, R43604, Jun 17, 2014. https://fas.org/sgp/crs/homesec/R43604.pdf.

[Paul W. Parfomak is an energy and infrastructure policy specialist. Report details vulnerability of US electric grid, with emphasis on transformer risk.]

U.S. CONGRESS STAFF (Markey): Fukushima Fallout: Regulatory Loopholes At U.S. Nuclear Plants, Congressman Edward J. Markey Staff Report, May 12, 2011. http://www.hsdl.org/?view&did=5112.

[Report prepared by the staff of Rep. Edward J. Markey (D-MA) summarizing failings of the NRC schema to protect against vulnerabilities exposed by the Fukushima disaster. Areas of focus are: emergency diesel generator failures (decades of reliability and maintenance problems); spent fuel vulnerabilities (including lack of emergency power backup); earthquake risk; and hydrogen explosion risks.

From 2002 to 2010, there were at least 69 reports of emergency diesel inoperability affecting 48 reactors, including 19 failures lasting over 2 weeks and 6 that lasted longer than a month. Among the failures in New York: At Indian Point 2 emergency diesel generators were rendered inoperable during a March 2010 refueling shutdown due to the inadvertent isolation of service water cooling caused by the failure to properly verify the in-service cooling header. Two of the 3 emergency diesel generators at Indian Point 2 were rendered inoperable in Oct 2002 because of component failure conditions expressly prohibited by tech specs. At the Fitzpatrick plant, emergency diesel generators were rendered inoperable in Jul 2009 due to degraded voltage timers. (Table 2, pp 25 – 28)

Indian Point and Pilgrim are the nuclear plants in the central and eastern US a NRC post-Fukushima staff review found most at-risk of core damage from earthquakes. Analysis of seismic data from a 2008 US Geological Survey revealed core damage risk to Indian Point to be 72% higher than previously believed. (p 19) The post-Fukushima NRC staff analysis also showed that the commission lacks detailed information on the physical vulnerability of about a third of US nuclear reactors.

Further, the “estimated national frequency of reactor core damage due to earthquakes does not factor in the additional hazards due to events that are independent of earthquakes, such as strong storms, wind, fires, operator error, reactor aging issues (for example, failures due to the corrosion of buried pipes that transport both cooling water and fuel to the emergency diesel generators and submerged cables), or terrorism.” (p 20)]

U.S. DEPARTMENT OF ENERGY (DOE): U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather, U.S. Department of Energy report, Jul 11, 2013. http://energy.gov/sites/prod/files/2013/07/f2/20130710-Energy-Sector-Vulnerabilities-Report.pdf.

[Report assesses the vulnerability of critical energy and electricity infrastructure to climate change. Climate change is being accompanied by droughts, heat, wildfires, and floods, and intense storms.

"Changes in climate have the potential to significantly impact U.S. energy security by forcing the present aging energy system to operate outside of the ranges for which it was designed." (p 1) Vulnerabilities in the energy sector are both acute and chronic. Existing barriers in the energy sector include "[l]imited understanding of vulnerabilities based on their probability and significance." (p 6)

The implications for America's energy infrastructure include the increased risk of temporary partial or full shutdowns at nuclear, coal, and natural gas thermoelectric power plants because of higher ambient air and water temperature and decreased water availability for cooling. Examples: In August 2012, a reactor at the Millstone Nuclear Power Station in Connecticut shut down because the intake cooling water of the Long Island Sound was too high, exceeding the technical specifications of the reactor. In July 2012, 8 plants (4 nuclear and 4 coal) in Illinois were forced to get special exemptions from state regulators to operate with water temperature discharge levels in excess of Clean Water Act permits. In September 2011, high temperatures and high electricity demand-related loading tripped a transformer and transmission line in Arizona starting a chain of events that led to the shutting down of the San Onofre nuclear power plant in California. In 2011, 2010 and 2007, the Browns Ferry Nuclear Plant in Alabama had to reduce power because the temperature of the Tennessee River water was too high. In 2010, the Hope Creek Nuclear Generating Station in New Jersey and the Limerick Generating Station in Pennsylvania had to reduce power because temperatures of the intake cooling water from the Delaware and Schuylkill Rivers were too high and did not provide sufficient cooling. In August 2006, two nuclear reactors at the Quad Cities Generating Station in Illinois had to reduce production because the temperature of the Mississippi River was too high to discharge heated cooling water. In July 2006, a D.C. Cook Nuclear Plant reactor was shut down because the temperature of the cooling water from Lake Michigan was too high to intake for cooling and the air temperature inside the containment building rose above 120°F.

Climate change brings increasing risk of physical damage to electricity distribution systems from hurricanes, storms, storm surges and flooding increased risks to energy infrastructure located along the coast from sea level rise, increasing intensity of storms, and higher storm surges and flooding. Disruption can be to both electricity and fuel production and distribution. Examples:

- In February 2013, over 660,000 customers lost power across 8 states in the Northeast affected by a winter storm that delivered snow, heavy winds, and coastal flooding. There was significant damage to the regions electric transmission system.

- In October 2012, "storm surge and high winds from Hurricane Sandy downed power lines, flooded substations and underground distribution systems, and damaged or temporarily shut down ports and several power plants in the Northeast, including all nuclear power units in the region. More than 8 million customers in 21 states lost power as a result of the hurricane, and fuel pumps at gas stations were not working due to power outages and lack of backup generation." (p 30)

- In June 2012, nearly 3 million people and businesses lost power because of complexes of thunderstorms coupled with strong winds that swept across the Midwest to the Mid-Atlantic coast. Storms also damaged a Maryland water plant resulting in imposition of water restrictions.

- In July 2011, a buried ExxonMobil pipeline was torn apart by flood-caused debris. In June 2011, Missouri River floodwaters surrounded the (offline) Fort Calhoun Nuclear Power Plant in Nebraska. Floodwaters persisted during the summer.

- In 2005, Hurricanes Katrina and Rita inflicted significant damage on the Gulf Coast.

- In September 2004, Hurricane Jeanne shut down several power plants and damaged power lines in Florida resulting in the loss of electrical service for nearly 2.6 million customers.

Wildfires are growing more intense and frequent and large. Wildfire season has increased by nearly 80 days over the past three decades and the average duration of large fires has almost quadrupled to 37 days. All these factors are bringing with them increased risk of fire damage to electricity distribution systems. Examples: During the summer of 2011, severe drought and record wildfires in Arizona and New Mexico burned more than a million acres and threatened the US Department of Energy's Los Alamos National Laboratory as well as two high voltage lines transmitting electricity from Arizona to about 400,000 customers in New Mexico and Texas. In October 2007, wildfire damage to the Southwest Power link transmission system in California damaged some 35 miles of wire.

The grid is also vulnerable to hot temperatures. For example heat-caused power disruptions occurred during the summer of 2006 when electric power transformers failed in California, Missouri and New York. Hot temperatures can also cause thermal expansion and the sagging of overhead transmission lines. A relatively small increase in thermal expansion can produce significant increase in sag. "This can pose many risks, including fire and safety hazards, and increased chance of power outages due to lines contacting trees or the ground." (p 13)]

U.S. DEPARTMENT OF ENERGY (DOE): U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather, U.S. Department of Energy, DOE/PI-0013, Jul 2013. http://energy.gov/sites/prod/files/2013/07/f2/20130716-Energy%20Sector%20Vulnerabilities%20Report.pdf.

[The US Department of Energy report assesses the vulnerability of U.S. critical energy and electricity infrastructure to the impacts of climate change. In recent years, widespread and long droughts, extreme heat waves, more severe and prevalent wildfires, and intense storms that caused power and fuel disruptions for millions have occurred and these trends are expected to continue.

Increasing risks include temporary partial or full shutdowns at nuclear power plants because of decreased water availability for cooling and higher ambient and air water temperatures.

Risk to infrastructure located along the coast is increasing due to sea level rise, increasing intensity of storms, and higher storm surge and flooding. Water levels of rivers may be affected by both drought and flooding. Distribution systems for gasoline may be disrupted. Climate change, additionally, poses increasing risk of physical damage to power lines, transformers and electricity distribution systems from hurricanes, storms and wildfires that are growing more intense and more frequent.]

U.S.DEPARTMENT OF ENERGY (DOE): Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security, Audit Report of the U.S. Department of Energy Office of Inspector General Office of Audits and Inspections, Jan 2011, DOE/IG-0846. http://energy.gov/sites/prod/files/igprod/documents/IG-0846.pdf.

[The DOE Inspector General reports that the security of the nation's power grid continues to be an area of critical concern. Testimony before Congress disclosed significant vulnerabilities in the power grid's infrastructure.

"Without improving its authority and oversight process related to protecting the Nation's power grid, the Commission may be unable to ensure that cyber security vulnerabilities are mitigated or that the effects of weaknesses are minimized. The current Administration and intelligence officials have expressed concerns over security for the Nation's power grid, noting that intruders have probed the power grid and cyber attacks have occurred against electrical and other critical infrastructure elsewhere. In addition, industry representatives indicated that, although becoming more streamlined, both the current standards and those in development cannot address advanced persistent threat attacks against the power grid." (p 10)

"In addition, the Department of Energy's (Department) Idaho National Laboratory, in conjunction with the Department of Homeland Security, recently illustrated that a cyber attack upon a power grid generator could potentially cause it to self-destruct. This experiment, called the Aurora Project, demonstrated how efforts to transfer control of generation and distribution equipment from internal networks to systems that could be accessed through the Internet have opened the power grid to additional cyber security vulnerabilities. Furthermore, a Department report recently identified many vulnerabilities with systems supporting the Nation/s critical infrastructure, including weaknesses ...such as missing software security patches and weak password management." (pp 10-11)

"In addition, as noted in a recent survey conducted by industry and the Center for Strategic and International Studies, more than half of the operators of power plants and other 'critical infrastructure' components reported that their computer networks had been infiltrated by sophisticated adversaries. Furthermore, during recent testimony to Congress, the Director of National Intelligence stated that the cyber security threat was growing at an unprecedented rate ....[Cyber security vulnerability] was recently highlighted by the discovery of sophisticated malware within various industrial control systems. An industry expert also noted that there have been more than 125 industrial control system incidents resulting in impacts ranging from environmental and equipment damage to death." (p 11)]

U.S. DEPARTMENT OF ENERGY - PIPELINE AND HAZARDOUS SAFETY ADMINISTRATION (PHMSA): U.S. Department of Energy Pipeline and Hazardous Safety Administration web page, accessed May 19, 2015. http://www.phmsa.dot.gov/

[There were 119 incidents in gas transmission pipelines in the US.]

U.S. ENERGY REGULATORY COMMISSION: McClelland, Joseph Testimony, 2012: Testimony of Joseph McClelland, Director, Office of Electric Reliability, Federal Energy Regulatory Commission Before the Committee on Energy and Natural Resources, United States Senate, Jul 17, 2012. http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=142d2c6c-e7e3-4b3b-9084-c7ef4ab4b88c.

[Joseph McClelland, Director of the Office of Electric Reliability, Federal Energy Regulatory Commission testifies that the Federal Energy Regulatory Commission (FERC) does not have sufficient jurisdiction or authority to address the full spectrum of vulnerabilities of or threats to the nation's electrical infrastructure. Notably, the current interpretation of "bulk power system" is limited and, for instance, "excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas." (p 2)

The current regulatory process operates too slowly to address emerging cyber threats and procedures "do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations." (p 4)

"The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks …. One example of a physical threat is an electromagnetic pulse (EMP) event. EMP events can be generated from either naturally occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents. This effect, also termed the 'E3' component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area." (p 5) EMP can also be generated by weapons. "Equipment and plans are radily available that have the capability to generate high-energy bursts, termed 'E1', that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets." (p 5)]

U.S. FEDERAL ENERGY REGULATORY COMMISSION (FERC): McClelland, Joseph Testimony, 2012: Testimony of Joseph McClelland, Director, Office of Electric Reliability Federal Energy Regulatory Commission Before the Committee on Energy and Natural Resources, United States Senate, Jul 17, 2012. http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=142d2c6c-e7e3-4b3b-9084-c7ef4ab4b88c.

[The Federal Energy Regulatory Commission (FERC) does not have sufficient jurisdiction or authority to address the full spectrum of identifies vulnerabilities of or threats to the nation's electrical infrastructure.

Notably, the current interpretation of "bulk power system" is limited and, for instance, "excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas." (p 2)

The current regulatory process operates too slowly to address emerging cyber threats and procedures "do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations." (p 4)

"The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks …. One example of a physical

threat is an electromagnetic pulse (EMP) event. EmP events can be generated from either naturally occurring or man-made causes. In the case of the former, solar magnetic disturbances periodically disrupt the earth's magnetic field which in turn, can generate large induced ground currents. This effect, also termed the 'E3' component of an EMP, can simultaneously damage or destroy bulk power system transformers over a large geographic area." (p 5)

The power grid is vulnerable to major solar storm such as those which occurred in 1859, 1921, and 1960. A March 2010 study from Oak Ridge National Laboratory and Metatech, commissioned by federal regulators, detailed the risks involved. "The results of the study support the general conclusion that EMP event pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years." (p 6)

EMP can also be generated by weapons. "Equipment and plans are readily available that have the capability to generate high-energy bursts, termed 'E1', that can damage or destroy electronics such as those found in control and communication systems on the power grid. These devices can be portable and effective, facilitating simultaneous coordinated attacks, and can be reused, allowing use against multiple targets." (p 5)]

U.S. GOVERNMENT ACCOUNTABILITY OFFICE: Wilshusen, Gregory C, Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies, Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps, Testimony of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office, GAO-15-758T, Jul 8, 2015. http://www.gao.gov/assets/680/671253.pdf.

[Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal and nonfederal systems and operations…in the past year, there has been a dramatic increase in malicious cyber activity targeting U.S. computers and networks…." (p 1) Electrical infrastructure has already been targeted. Threats to the nation's critical infrastructure include actions by not just foreign nations engaged in espionage and information warfare, but criminals, hackers, virus writers, and disgruntled employees and contractors.]

U.S. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (9/11 COMMISSION): Final Report of the National Commission on Terrorist Attacks Upon the United States: The 9/11 Commission Report, W.W. Norton & Company, New York, London, Jul 2004. http://www.9-11commission.gov/report/911Report.pdf.

[The 9/11 Commission Report provides an exhaustive and authoritative narrative of the events which led up to the terrorist attack of Sep 11, 2001. It describes multiple failures at multiple

levels of government, as well as lax security at commercial airports and in commercial airlines. It famously notes a “failure of imagination.”

The 9/11 Commission Report also attests that America’s nuclear power plants are viewed as terrorist targets. The original plan, as described by Khalid Sheikh Mohammed (SDM), the Pakistani mastermind of the attack, was “a total of ten aircraft to be hijacked, nine of which could crash into targets on both coasts – they included those eventually hit on September 11 plus CIA and FBI headquarters, nuclear power plants, and the tallest buildings in California and the state of Washington.” (p 154)

Two of the terrorists who ultimately piloted the planes, did practice and training flights down the Hudson Corridor, a low-altitude hallway along the Hudson River. (p 242)

A planning meeting for the attacks took place in Madrid on July 8, 2001. Mohamed Atta, the Egyptian tactical leader of the plot and pilot of the lead plane, American Airlines Flight 11, was in attendance. “During the Spain Meeting, Atta also mentioned that he had considered targeting a nuclear facility he had seen during familiarization flights near New York – a target they referred to as ‘electrical engineering.’” (p 245)]

U.S. NATIONAL TRANSPORTATION SAFETY BOARD (NTSB): Natural Gas-Fueled Building Explosion and Resulting Fire New York City, New York March 12, 2014, National Transportation Safety Board Accident Report NTSB/PAR-15/01, PB2015-104889, Jun 9, 2015. http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR1501.pdf.

[On March 12, 2014, starting at about 9:30 am, a violent gas explosion and fire in East Harlem, New York City destroyed 2 buildings on Park Ave. Eight people died and more than 50 were injured. Gas likely started leaking from Con Ed’s system of underground pipes a day or so before the blast, then escaped through the ground into a 3 year-old plastic pipe, known as a service line.

The probable cause of the accident was the alignment of two factors: (1) improper welding and failure of a defective fusion joint at a service tee installed by Consolidated Edison (Con Ed) in 2011 that allowed gas to leak from the gas main and migrate into a building where it ignited and (2) a breach in a sewer line maintained by New York City that allowed groundwater and soil to flow into the sewer, resulting in a loss of support for the gas main, which caused the line to sag and overstressed the defective fusion joint.

A Con Ed contractor installed the service tee in 2011. Post-accident examination showed fracture features which indicated the surfaces were contaminated, resulting in a weak joint. Review of Con Ed’s procedure revealed some industry-standard steps – such as cleaning the surface with alcohol – were omitted. Bead sizes were also inconsistent.

In addition, at 9:06 am, about 25 minutes before the explosion, Con Ed received a call from a resident of an adjacent building who reported a gas odor and said the gas was coming from one of the buildings later destroyed in the accident. During the call, the Con Ed customer service representative’s computer stopped responding (was “freezing”), which delayed the notifications. At about 9:19 am, the dispatcher called the New York City Fire Department (FDNY) to report the possibility of a gas order but said, “’Hold up, no, sorry, hold on one second, hold on, hold on, I’ll

call you right back.'" (p 3) But the operations dispatcher failed to call The FDNY back. A Con Ed mechanic was directed to respond to the area but he arrived at 9:39 am, a few minutes after the explosion.

The explosion prompted numerous 911 calls to the FDNY and the first fire engine from a nearby station arrived at the scene a few minutes after the first 911 call, but did not receive notice of the gas leak until after the building exploded and was on fire. This release notified Had Con Ed notified the fire department when the call to the service rep ended, NYFD could have arrived at the gas leak location up to 15 minutes before the explosion. However it is unclear whether emergency responders could have evacuated the two 5-story buildings that were not equipped with elevators or fire alarm systems.

Con Ed was unable to turn off the gas to the leaking pipeline until 1:44 pm, more than 4 hours after the explosion.

Investigators also found a large breach in the sewer main near the destroyed buildings which had gone unrepaired for more than 8 years. A few days before the accident, major street repair work was done to correct significant ground settling below the pavement in the vicinity of the gas main and building service lines.

The NTSB further found that NY state pipeline safety regulations were less stringent than federal regulations in the areas of definition of service line and pipeline pressure testing – deficiencies not identified by the federal Pipeline and Hazardous Materials Safety Administration during state program recertification. Moreover the NYS Department of Public Service audit program for pipeline operators does not effectively address all aspects of the state regulations.

Occurrences and factors noted included: (i) A water main break ensued. This most likely resulted when the pipe, weakened by corrosion, was shaken by the gas explosion shock wave or from increased loading from the incident response equipment. (ii) Supporting soil under the gas and water mains was washed into the sewer through a hole in the sewer wall over many months or years when groundwater accumulated. (iii) As the soil washed away after the 2011 plastic gas main and service tee installation, the main was no longer supported in the tee vicinity, causing the line to sag and overstressing the defective fusion joint at the tee. (iv) Local soil movement and settlement caused by the localized groundwater movement damaged the street. Had NYC repaired the sewer main breach after it was discovered in 2006, damage to the street would been prevented. (v) The surfaces of the service tee outlet and gas main were not adequately prepared before the tee was fusion welded to the gas main in 2011, resulting in a defective fusion joint; ie, incomplete fusion. (vi) Visual inspection to confirm the requisite number of beads would not provide sufficient evidence of a properly welded joint. (vii) Stresses caused by the vertical displacement of the sagging gas main opened a crack in the defective service tee fusion joint, allowing natural gas to escape into the subterranean area and migrate. (viii) Had Con Ed installed appropriately located isolation valves on the gas distribution main, the leaking gas main could have been isolated sooner following the explosion. This would have reduced the danger to the first responders as well as the delay in recovery operations.

The "violent explosion" also damaged buildings in the vicinity other than the ones destroyed. Metro-North Railroad was forced to suspend rail service for about 7 ½ hours on the elevated railway along Park Avenue because of debris from the explosion on the track.

Con Ed had developed and maintains emergency plans and conducts numerous drills, but failed to follow its own procedure during the incident.]

U.S. NATIONAL TRANSPORTATION SAFETY BOARD (NTSB): Pacific Gas and Electric Company Natural Gas Transmission Pipeline Rupture and Fire San Bruno, California September 9, 2010. National Transportation Safety Board (NTSB) Accident Report, NTSB/PAR-11/01; PB2011-916501, Aug 30, 2011. http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR1101.pdf.

[On September 9, 2011, a 30 inch diameter segment of an intrastate natural gas transmission pipeline in San Bruno, California, owned and operated by Pacific Gas and Electric Company (PG&E), ruptured. The rupture occurred at 6:11 pm; "almost immediately, the escaping gas from the ruptured pipe ignited and created an inferno." (p x) It took PG&E 95 minutes to stop the flow of gas and isolate the rupture site.

The rupture produced a crater about 72 feet long by 26 feet wide. The section of pipe that ruptured – which was about 28 feet long and weighted about 3,000 pounds – was found 100 feet south of the crater. PG&E estimated that 47.6 million standard cubic feet of natural gas was released. The released gas ignited, causing a fire that destroyed or damaged 108 homes, killed 8 people and injured 58 others.

By 6:24 pm, firefighters responding to the south side of the accident area reported that hydrants were dry. Firefighters responding to the north side discovered the explosion had damaged a water line. The firefighters jury rigged hose connections.

At 6:27, a PG&E dispatcher called the PG&E SCADA center to ask the operator if the center had observed a gas pressure drop at a station in the San Bruno area. The dispatcher replied that he had received reports of a flame accompanied by a sound similar to a jet engine. "Reports of a plane crash, a gas station explosion, or some combination fo the two persisted throughout the initial hours of the emergency response." (p 14) By 6:30 p.m., some staff at the SCADA center realized that there had been a gas line rupture, but did not know the exact location.

At 6:35 pm, an off-duty PG&E gas measurement and control mechanic saw media reports about the fire. He suspected a gas transmission line break and notified the PG&E dispatch center, then he proceeded to the PG&E Colma yard to obtain his service truck and the tools necessary to shut off mainlines – while en route, he received a call from a supervisor directing him to the yard with a second mechanic.

Meanwhile, another PG&E supervisor who lived about 4 miles from the rupture site learned of the explosion and fire through media reports and notified the PG&E SCADA center. The PG&E supervisors arrived on the scene at ~6:41 pm, but "none of these three PG&E first responders were qualified to operate mainline valves." (p 15) The PG&E operations emergency center in San Carlos was activated by about 6:55 pm.

The PG&E mechanics with the ability to close valves arrived at the first valve location by 7:20 pm. At 7:22 pm, one of the PG&E supervisors on the scene contacted the PG&E dispatch center to covey that "although it was still unconfirmed, the incident was likely a reportable gas

fire." (p 16) By 7:46 pm mechanics with assistance from a supervisor were able to manually close the valves and isolate the ruptured section of pipe. By 11:32 pm, PG&E crews were able to manually close 2 distribution line valves and pinch 3 more distribution lines using hand tools to stop the gas-fed house fires surrounding the pipeline rupture. "Although the gas flow through the transmission line break and several local distribution lines had been stopped, the resulting fire continued." (p 18) The fire was declared about 75% contained by 4:24 am on September 10, 2011 - about 10 hours and 13 minutes after the pipe rupture – however fire operations continued to extinguish fires and monitor hot spots until about 8:00 pm on September 11, 2011.

During the 50 hours following the accident, some 600 firefighting and medical service personnel and 325 law enforcement personnel responded. Firefighting efforts included air and forestry operations. The fire damage extended to a radius of about 600 feet from the pipeline blast center. A professional meteorologist familiar with the local terrain and micro-climates estimated wind speeds during the 6:00 – 9:00 pm period between 15-20 mph.

The NTSB investigation blamed PG&E for a poor safety practices. Inadequate quality assurance and control decades earlier had resulted in installation of a substandard and poorly welded pipe section. Over time, the seam weld flaw grew via two different modes. The crack first grew by ductile fracture (in which the metal ahead of the crack undergoes deformation prior to crack advancement) starting at the root of the weld. Subsequently, it grew by fatigue fracture (associated with alternating stresses in which the crack advances with each alternating stress cycle). Crack propagation ultimately advanced until the crack finally ruptured. An inadequate pipeline integrity management program then failed to detect and repair or remove the defective pipe section.

Lax oversight on the part of the state regulators and the U.S. Department of Transportation's grant of exemptions of existing pipelines from the regulatory requirement for pressure testing contributed to the accident (known as a "grandfather clause" (p 34) .

Contributing to the severity of the accident and increasing the life-threatening risks to the community and first responders, was the lack or either automatic shutoff valves or remote control valves on the line, PG&E's flawed emergency response procedures and delay in isolating the rupture to stem the flow of gas. PG&E's SCADA center (located at the corporate headquarters in San Francisco) managed operations of the utility's gas transmission pipeline system. The center was staffed by 3 SCADA operators during the day shift (6:00 am- 6:00 pm) and 2 night shift operators (6:00 pm – 6:00 am) + 2 coordinator personnel during all shifts. "Company Gas Emergency Plan" graphic of emergency response procedure figure 23, p 55)

Deficiencies revealed by this NTSB investigation were previously revealed in the NTSB's investigation of the 2008 explosion of a PG&E gas pipeline in Rancho Cordova, California. Some of these same deficiencies were also found by the NTSB's investigation of a 1981 PG&E gas pipeline leak in San Francisco.]

U.S. NUCLEAR REGULATORY COMMISSION (NRC): Transcript of Nuclear Regulatory Commission Proceedings, 10 CFR 2. 206 Petition Review Board Re Indian Point Nuclear Generating Unit, Docket No. 05000247 and 05000286, Jan 28, 2015. https://sape2016.files.wordpress.com/2013/11/prb-transcript-1-28-2015-2-2.pdf.

[Paul M. Blanch, PE, an engineer who once worked as a consultant at Indian Point, raises concern about the pipeline risk.]

U.S. NUCLEAR REGULATORY COMMISSION (NRC): NRC ANO Augmented Inspection Team Report, 2013: U.S. Nuclear Regulatory Commission Augmented Inspection Team Report 05000313/2013011 and 05000368/2013011, Jun 7, 2013. http://www.nucpros.com/content/arkansas-nuclear-one-nrc-augmented-inspection-team-report-june-7-2013 http://pbadupws.nrc.gov/docs/ML1315/ML13158A242.pdf.

[Spent fuel pool cooling was lost and had to be restored manually during a March 31, 2013 accident at Arkansas Nuclear One Units 1 and 2 operated by Entergy Operations Inc under the aegis of Entergy Arkansas, Inc.

Accident occurred on Easter Sunday morning during a refueling outage. A temporary overhead crane being used to move a 525 ton stator fell, heavily damaged structures, killed a worker and injured 8 others. All offsite power to Unit 1 was lost due to damage from the fallen stator. The loss of offsite power led to the loss of power to both decay heat removal trains (which were then restored manually. The impact of the crane components on the turbine deck caused electrical breakers to open, removing power from a reactor cooling pumps at Unit 2. A fire main ruptured. Water pouring from the fire main rupture caused a short circuit and small explosion inside an electrical breaker cabinet at Unit 2. This, in turn, led to the loss of an offsite power source to Unit 2. The inspectors – reporting here on a May 9, 2013 inspection – noted damage to "Unit 1 and Unit 2 Structures, Systems and Components".]

U.S. NUCLEAR REGULATORY COMMISSION (NRC): Consequence Study of a Beyond-Design-Basis Earthquake Affecting the Spent Fuel Pool for a U.S. Mark I Boiling Water Reactor, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Oct 2013. http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2013/2013-0112scy.pdf.

U.S. NUCLEAR REGULATORY COMMISSION (NRC): A Summary of Aging Effects and Their Management in Reactor Spent Fuel Pools, Refuelling Cavities, TORI and Safety-Related Concrete Structures, U.S. Nuclear Regulatory Commission study, NUREG/CR-7111 (2011). http://pbadupws.nrc.gov/docs/ML1204/ML12047A184.pdf,

U.S. NUCLEAR REGULATORY COMMISSION (NRC): On Site Spent Fuel criticality Analyses, NRR Action Plan, U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation memo, May 21, 2010. http://pbadupws.nrc.gov/docs/ML1015/ML101520463.pdf.

[NRC staff memo expressing concern over a possible inadvertent criticality event due to the buildup of spent fuel in pools. The lack of a permanent disposal option has led to the re-racking of spent fuel assemblies in closer proximity to one another. "The conservatism/margins in spent fuel pool (SFP) criticality analyses have been decreasing…Fuel assemblies themselves have become more reactive. Increased U235 enrichment is an obvious example…The new rack designs rely heavily on permanently installed neutron absorbers to maintain criticality

requirements. Unfortunately, virtually every permanently installed neutron absorber, for which a history can be established, has exhibited some degradation. Some have lost a significant portion of their neutron absorbing capability. In some cases, the degradation is so extensive that the permanently installed neutron absorber can no longer be credited in the criticality analysis." (p 1)]

U.S. SENATOR SCHUMER: Schumer, Charles E, letter to Richard A Meserve, Chairman, Nuclear Regulatory Commission, Dec 10, 2002. http://pbadupws.nrc.gov/docs/ML0235/ML023500149.pdf.

[NY Senator Charles E. Schumer urges Nuclear Regulatory Commission (NRC) Chairman Richard A. Meserve to "launch an immediate investigation" into the capability of Indian Point to defend against terrorist attack. "As I'm sure you are aware," the Senator writes, "a report commissioned by the owners of Indian Point has identified serious security deficiencies at the facility." He continues:

"According to the report, as many as half of the security personnel at Indian Point's Unit 2 nuclear reactor may be unable to physically meet the demands of defending the plant, and physical evaluations of security personnel are exceedingly lax. The report also alleges that guards are hired with little experience and almost no relevant qualifications. Additionally, there are indications that guards are minimally trained and equipped, and that some have been hired despite the fact that they required multiple attempts to pass their weapons tests. The report also said that guards at Indian Point regularly work 70-80 hours per week."

"While these revelations are disturbing, they pale in comparison to the report's suggestion that force-on-force exercises intended to evaluate Indian Point's ability to defend against a terrorist attack were manipulated to ensure that the mock attacks would not be successful. In addition, there are indications that guards working at Indian Point feel that they are operate [sic] in a 'chilled' atmosphere where reports of security deficiencies are suppressed, and the identification of security flaws is discouraged. In fact, some personnel are concerned that blowing the whistle on security problems could result in their termination."

Sen. Schumer stresses that the consequences of a successful terrorist attack on Indian Point – with 20 million people living within the reactors' 50 mile radius – would be "catastrophic".

"A terrorist attack on the facility could have devastating consequences and could render the New York City metro area uninhabitable."]

VICE: Dyer, John, Giant Gas Pipeline Next to nuclear Power Plant Could Cause a New York 'Fukishima,' Say Experts, VICE News, May 21, 2015. https://news.vice.com/article/giant-gas-pipeline-next-to-nuclear-power-plant-could-cause-a-new-york-fukishima-say-experts.

[Paul Blanch, a retired engineer with decades of experience in nuclear safety, warns that a massive natural gas pipeline being constructed next to the Indian Point nuclear power plant in New York could cause a meltdown. Spectra Energy has started construction on a 42-inch-diameter pipeline that will pass only 105 feet from the 1970s-era Indian Point nuclear facility on

the Hudson River in Buchanan, New York. If this pipe ever exploded, Blanch said, it could damage two diesel fuel tanks and a switching station that provide power for the nuclear plant.

"'We would have a total loss of power and would wind up with exactly what happened at Fukushima,' Blanch told VICE News. 'Fukushima didn't melt down because of the tsunami. They melted down because they didn't have power.'

"A recent fire at Indian Point following the explosion of a transformer — the third transformer failure in eight years — has heightened concerns that safety measures and inspections are inadequate."]

WALL STREET JOURNAL: Iranian Hackers Infiltrated New York Dam in 2013, Wall Street Journal, Dec 21, 2015. http://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559.
[Iranian hackers infiltrated the control system of the Bowman Avenue Dam, a small dam used for flood control near Rye, NY in Westchester in 2013. The hackers were believed to have gained access to the dam through a cellular modem, according to an unclassified Homeland Security summary.

"The still-classified dam intrusion illustrates a top concern for U.S. officials as they enter an age of digital state-on-state conflict." America's power grid, plants, pipelines, bridges and dam water release systems are all prime cyber targets. Unlike traditional attacks, it can be difficult to know whether or where a cyberattack has struck. In the case of the Westchester dam probe, federal investigators were at first unable to determine where the hackers had infiltrated. They initially thought the target might have been a much larger dam in Oregon."

"The incident at the New York dam was a wake-up call for U.S. officials, demonstrating that Iran had greater digital-warfare capability than believed and could inflict real-world damage, according to people familiar with the matter."

The dam sits less than 20 miles from New York City. The breach came amid other attacks linked to Iran a few years after the US launched an attack against the Natanz Iran nuclear facility with a sophisticated computer worm called Stuxnet. The Stuxnet virus unintentionally self-replicated and spread to other networks, including systems at Chevron.

The US has more than 57,000 industrial control systems connected to the Internet, according to Shodan, a search engine that catalogs systems online. They range from office air conditioning systems to major electric, pipeline, dam, and traffic control systems. Hackers could theoretically set off an explosion, flood or traffic jam. For the 12 months ended September 30, 2015, The Department of Homeland Security had received reports of 295 industrial control system hacking incidents. Most involved system probes.

In the winter of 2014, hackers broke into the control system of a German steel plant and caused massive damage to a blast furnace. At a Las Vegas hacker conference later that year, Cesar Cerrudo, Chief Technology Officer at the security firm IOActive Labs, demonstrated how he could manipulate the traffic lights of major US cities.]

WALL STREET JOURNAL: Yadron, Danny, Three Months Later, State Department Hasn't Rooted Out Hackers, Wall Street Journal, Feb 20, 2015. http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453.

[Three months after the officials confirmed digital espionage of State Department email networks, the government remains unable to disable the malware. Investigators believe hackers first gained access via a phish attack in the fall of 2014 when an employee clicked on a fake link in an email referencing administrative matters. From there the malicious software spread through the State Department's vast network which encompasses thousands of domestic government offices, embassies and other outposts.

The intrusion software is similar to a fall 2014 breach of the White House's unclassified email system which some US officials deem linked to Russia. Hacking into US Navy network was discovered in 2013 and took about 4 months to cleanup. The State Department, White House and Navy attacks involved systems which were unclassified, but nevertheless sensitive.

Penetration into a classified network of the US Central Command in 2008 took the Defense Department about a month to disable.]

WORLD AFFAIRS JOURNAL: Woolsey, R James, Rachel Kleinfeld and Chelsea Sexton, No Strings Attached: The Case for a Distributed Grid and a Low-Oil Future, World Affairs Journal, Sep-Oct 2010. http://www.worldaffairsjournal.org/article/no-strings-attached-case-distributed-grid-and-low-oil-future.

[World Affairs is a highly regarded foreign policy and international affairs journal. R. James Woolsey, a former CIA Director, is chair of Woolsey Partners. Rachel Kleinfeld is co-founder and CEO of the Truman National Security Project. Chelsea Sexton is the founder of the Lightning Rod Foundation.

Energy policy affects a wide range of issues, from national security to international corruption to economics to climate change pollution and public health – and all must all be taken into account. The demand for new energy solutions worldwide is vast and will create a huge market. The challenge is to find available and scalable solutions that resolve complicated problems in interconnected systems without causing inadvertent side effects. "Therefore, we believe it is necessary to find answers that at best alleviate multiple problems, and, at worst, don't exacerbate one problem while curing another."

Energy decisions should take into account security threats, environmental and health quality-of-life issues, and environmental justice, as these are all often interdependent. Environmental stresses can cause security problems and environmental degradation can make life worse for the poor. The need is not to search for a single solution, but for a portfolio of options that together meet these key concerns; as well as solutions that can begin working immediately.

"With regard to electricity, our investigation has led us to conclude that distributed generation—including a disaggregated grid that produces electricity close to where it is consumed and that can 'island' to support small communities while securing itself from cascading grid failure—is key to solving the complex mix of energy problems we face. Such distributed generation would

rely more heavily on local facilities producing energy from renewables such as solar, wind, and geothermal power, with a significant role for natural gas as a baseload that could 'firm' or supplement the other, intermittent sources."

America operates from two almost completely disconnected energy systems: a transportation network fueled by oil and largely coal-based electrical grid. "We suggest a shift toward plug-in vehicles complemented by efficiency improvements to remaining internal combustion engines." Advanced biofuels and moving trucks and fleet vehicles to natural gas where electrification is less efficient are additional changes which are relatively simple to make within existing infrastructure without major technological breakthroughs.

The US electrical grid "is the security equivalent of a house left with the door unlocked, the windows open, and millions of dollars of jewelry and home entertainment equipment strewn about for the taking. If anyone wished to launch a national blackout, they could coordinate attacks in a few rural grassy fields, where major transformers are located. If enemies didn't want to bother with the travel, our grid is laughably open to cyber attack." An attack could take down water, sewage, phone, medical and transportation systems.

A priority should be to make the grid much more resilient, able to "island" into microgrids in the event of an outage, preventing a single failure from cascading into a catastrophe.

"The vast majority of homes and businesses would stay connected to the grid, but would harness solar, wind, geothermal, and other local renewable energy sources for an important share of their power needs. New policies would force utilities to allow a power payback system (i.e., a feed-in tariff), enabling individuals and commercial enterprises to sell the electricity they generate in excess of their own needs back to the grid and earn money on their investment. We would still have a national grid transferring bulk electric power over transmission lines on steel towers and via large transformers. We would simply build into our existing distribution grid the capability to island and separate when need be. (If the transmission lines are analogous to freeways, the distribution lines on telephones are the on- and off-ramps and local streets and roads.) Neighborhoods or towns would have the ability to cut themselves off from the rest of the grid if a major share of it were taken down by anything from a terrorist attack to falling tree branches. Micro-grids could provide many households, schools, and businesses with enough power to function during even a long-term emergency, rather than forcing populations to face the cascading total failure of lighting, plumbing, refrigeration, heating, and other infrastructure that an attack would cause today. By building resilience into our current grid, we could have both the benefits of a national grid system and the flexibility of distributed, independent generating capacity."

Neither nuclear power nor coal are desirable as backup baseload sources of power. Nuclear power generates nuclear waste and presents proliferation threat. Nuclear fuel is just a few cycles from weapons-grade fissile material. "In a number of countries, domestic producers of nuclear power plants are certain to try to export this technology." Burning coal produces large quantities of CO2 emissions, noxious chemicals, and mercury, as well as mining and mountaintop destruction. Consequently "natural gas is definitely the least of multiple evils when it comes to the required source of baseload power for a distributed generation future." Renewable energy expansion as rapidly as possible could enable the minimal amount of gas extraction. This would involve not just large solar plants and wind farms, but rapid expansion of small and medium-sized commercial renewable power facilities with capabilities of less than 20 MW. "To be commercially viable and create a market, utilities would need to allow entrepreneurs who install renewable energy platforms at a small commercial scale to sell their

electricity back to the grid." This change requires small infrastructure adjustments and rules that enable power payback, like feed-in tariffs, which enable businesses, farms, and homes to benefit from the electricity they produce and feed into the grid. Germany and 40 other countries have made this financing system work well.

Investment in energy conservation technologies is also crucial. Simple changes to building codes could, with today's technology, significantly reduce building energy use. Another priority is research and development of improved energy storage systems like batteries and compressed air energy storage (CAES) systems. Batteries are uniquely suited for microgrid support.

Decentralized grids and distributed energy are beneficial for advanced and developing countries. They can also reduce the leverage of dictatorships (which otherwise can could cut off electricity to any region that defies them).

Worldwide there are a multitude of distributed generation initiatives underway, from Kenya (where solar photovoltaic use in rural areas outpaces new grid connections and unsubsidized photovoltaics compose dominate the solar market) to inner Mongolia (where herdsmen can draw power from small wind turbines carried along with their portable yurt dwellings). More pilot projects need to be designed to enable a broad solution. However the promise is the call of the market. The world's poor, collectively, have significant purchasing power and represent a huge future entrepreneurial opportunity: the worldwide energy market for the poor is estimated to be worth some $230 billion.

National security concerns argue for moving away from energy technologies that subsidize hostile nations. America should also move away from ties to vulnerable supply lines that, if breached, could destroy our economy. As the security expert Anne Korin has observed, until the end of the 19th Century, salt was the only means of preserving meat. "Nations depended on it, and militaries marched for it. Countries that controlled salt mines wielded power and fought wars to control these strategic commodities." Then innovations like electricity and refrigeration broke salt's strategic importance, and it became a commodity like any other.

The same kind of transformation can be accomplish today via the strategy of electrifying a significant number of American household vehicles as in plug-in hybrids (PHEVs) and extended-range electric vehicles (EREVs). Where electrification is impractical, advanced biofuels and (reluctantly) natural gas could play a role.

Democracy is enhanced by distributed widely-available energy. Commodities that command huge amounts of economic rent tend to solidify concentrations of power. "Autocratic governments that need not depend on taxes for revenue have no need to enrich or serve their people. It's no surprise that of the top nine oil-exporting countries, only Norway is a democracy."

Whether the goals are security, the environment, or helping the poor, the shift to a new renewable and distributed energy model makes sense. "To power our electrical grid, combining renewables with the least harmful option of natural gas improves both security and environmental and health concerns. Retrofitting our grid to emphasize micro-grids and islanding will help reduce the brittleness of the current system. Cars should be electrified when practical, or fitted with greater efficiency improvements and fueled through drop-in advanced biofuels. These changes can all begin now, without the need to wait for major infrastructure overhauls or technological breakthroughs to get started."

“Distributed generation of fuels for both electricity and transportation offers America and the developing world a path toward self-reliance, transforming consumers into owners empowered with the means of production. A new energy posture could break the monopoly of oil-based autocracies and corrupt governments, diminish vulnerability to malevolent threats, and reduce the climate change, pollution, and health concerns that harm the quality of life worldwide.”]