UNITED STATES NUCLEAR REGULATORY COMMISSION
BEFORE THE EXECUTIVE DIRECTOR FOR OPERATIONS

In the Matter of:

SAPRODANI ASSOCIATES, and THOMAS SAPORITO **DATE: 18 OCT 2015**

Petitioner,

v.

ALL NRC LICENSEES,
(commercial nuclear power stations)

Licensee.
_____/

SUPPLEMENTAL PETITION UNDER 10 C.F.R. §2.206
SEEKING ENFORCEMENT ACTION AGAINST ALL NRC LICENSEES

NOW COMES, Saprodani Associates, by, through and with, Thomas Saporito, Senior Consultant for Saprodani Associates (hereinafter "Petitioner") and submits a "*Supplemental Petition Under 10 C.F.R. §2.206 Seeking Enforcement Action Against All NRC Licensees"* related to commercial nuclear power stations – (hereinafter "Petition"). For the reasons stated below, the U.S. Nuclear Regulatory Commission (NRC) should grant the Petition as a matter of law:

NRC HAS JURISDICTION AND AUTHORITY TO GRANT PETITION

The NRC is the government agency charged by the United States Congress to protect public health and safety and the environment related to operation of civilian commercial nuclear reactors in the United States of America (USA). Congress charged the NRC with this grave responsibility in creation of the agency through passing the Energy Reorganization Act of 1974 (ERA). In the instant action, the above-captioned entity(s) is/are collectively and singularly a "licensee" of the NRC and subject to NRC regulations and authority under 10 C.F.R. §50 and under other NRC regulations and authority in the operation of one or more nuclear reactors. Thus, through Congressional action in creation of the agency; and the fact that the named-actionable party identified above by Petitioner is collectively and singularly a licensee of the NRC, the agency has jurisdiction and authority to grant the Petition.

STANDARD OF REVIEW

A. Criteria for Reviewing Petitions Under 10 C.F.R. §2.206

The staff will review a petition under the requirements of 10 C.F.R. §2.206 if the request meets all of the following criteria:

- The petition contains a request for enforcement-related action such as issuing an order modifying, suspending, or revoking a license, issuing a notice of violation, with or without a proposed civil penalty, etc.

- The facts that constitute the basis for taking the particular action are specified. The petitioner must provide some element of support beyond the bare assertion. The supporting facts must be credible and sufficient to warrant further inquiry.

- There is no NRC proceeding available in which the petitioner is or could be a party and through which petitioner's concerns could be addressed. If there is a proceeding available, for example, if a petitioner raises an issue that he or she has raised or could raise in an ongoing licensing proceeding, the staff will inform the petitioner of the ongoing proceeding and will not treat the request under 10 C.F.R. §2.206.

B. Criteria for Rejecting Petitions Under 10 C.F.R. §2.206

- The incoming correspondence does not ask for an enforcement-related action or fails to provide sufficient facts to support the petition but simply alleges wrongdoing, violations of NRC regulations, or existence of safety concerns. The request cannot be simply a general statement of opposition to nuclear power or a general assertion without supporting facts (e.g., the quality assurance at the facility is inadequate). These assertions will be treated as routine correspondence or as allegations that will be referred for appropriate action in accordance with MD 8.8, “Management of Allegations”.

- The petitioner raises issues that have already been the subject of NRC staff review and evaluation either on that facility, other similar facilities, or on a generic basis, for which a resolution has been achieved, the issues have been resolved, and the resolution is applicable to the facility in question. This would include requests to reconsider or reopen a previous enforcement action (including a decision not to initiate an enforcement action) or a director's decision. These requests will not be treated as a 2.206 petition unless they present significant new information.

- The request is to deny a license application or amendment. This type of request should initially be addressed in the context of the relevant licensing action, not

under 10 C.F.R. 2.206.

- The request addresses deficiencies within existing NRC rules. This type of request should be addressed as a petition for rulemaking.

See, Volume 8, Licensee Oversight Programs, Review Process for 10 C.F.R. Petitions, Handbook 8.11 Part III.

REQUEST FOR ENFORCEMENT-RELATED ACTION TO MODIFY, SUSPEND, OR REVOKE A LICENSE AND ISSUE A NOTICE OF VIOLATION WITH A PROPOSED CIVIL PENALTY

A. Request for Enforcement-Related Action

Petitioner respectfully requests that the NRC: (1) take escalated enforcement action against the above-captioned licensee(s) and issue a Confirmatory Order to the licensee(s) requiring the licensee(s) to take their nuclear reactors and/or nuclear facilities to a “cold-shutdown” mode of operation until such time as:

1. The licensee completes an ***"independent"*** assessment to fully understand and correct the potential and/or realized security threat posed by outside organizations and/or individuals related to the operation of “drones” to attack the licensees' nuclear facility; and

2. The licensee completes a comprehensive evaluation of their nuclear security program as it relates to any potential and/or realized security threat posed by outside organizations and/or individuals related to the operation of “drones” to attack the licensees' nuclear facility; and

3. The licensee identifies and implements measures to correct any deficiencies in its security plan – related to any potential and/or realized security threat posed by outside organizations and/or individuals related to the operation of “drones” to attack the licensees' nuclear facility; and

4. The licensee completes an updated and approved physical security plan to the NRC which documents actions and measures in writing to be taken against any potential and/or realized security threat posed by outside organizations and/or individuals related to the operation of “drones” to attack the licensees' nuclear facility.

B. Facts That Constitute the Basis for Taking the Requested Enforcement-Related Action Requested by Petitioner

Since the development and retail sale of various types of “Drone” aircraft devices,

there have been serious violations committed by one or more individuals in the unauthorized operation of drones in areas strictly prohibited by law. Notably, drones have crashed on or near the White-house lawn. Moreover, various drones have interfered with wildfire fighting efforts and interfered with commercial aircraft operations. On at least one occasion, a college engineering student mounted a hand gun to a drone and was able to remotely discharge several rounds from the gun while the drone was airborne.

NRC regulations and requirements at 10 CFR 37.43 – state in part that:

(a) *Security plan.* (1) Each licensee identified in § 37.41(a) shall develop a written security plan specific to its facilities and operations. The purpose of the security plan is to establish the licensee's overall security strategy to ensure the integrated and effective functioning of the security program required by this subpart. The security plan must, at a minimum:

(i) Describe the measures and strategies used to implement the requirements of this subpart; and

(ii) Identify the security resources, equipment, and technology used to satisfy the requirements of this subpart.

(2) The security plan must be reviewed and approved by the individual with overall responsibility for the security program.

(3) A licensee shall revise its security plan as necessary to ensure the effective implementation of Commission requirements. The licensee shall ensure that:

(i) The revision has been reviewed and approved by the individual with overall responsibility for the security program; and

(ii) The affected individuals are instructed on the revised plan before the changes are implemented.

(4) The licensee shall retain a copy of the current security plan as a record for 3 years after the security plan is no longer required. If any portion of the plan is superseded, the licensee shall retain the superseded material for 3 years after the record is superseded.

(b) *Implementing procedures.*

(1) The licensee shall develop and maintain written procedures that document how the requirements of this subpart and the security plan will be met.

(2) The implementing procedures and revisions to these procedures must be approved

in writing by the individual with overall responsibility for the security program.

(3) The licensee shall retain a copy of the current procedure as a record for 3 years after the procedure is no longer needed. Superseded portions of the procedure must be retained for 3 years after the record is superseded.

(c) *Training.* (1) Each licensee shall conduct training to ensure that those individuals implementing the security program possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively.

C. There Is No NRC Proceeding Available in Which the Petitioner is or Could be a Party and Through Which Petitioner's Concerns Could be Addressed

Petitioner avers here that there is no NRC proceeding available in which the Petitioner is or could be a party and through which Petitioner's concerns could be addressed.

CONCLUSION

FOR ALL THE ABOVE STATED REASONS, and because Petitioner has amply satisfied all the requirements under 10 C.F.R. §2.206 for consideration of the Petition by the NRC Petition Review Board (PRB), the NRC should grant Petitioner's requests made in the instant Petition as a matter of law.[1]

Respectfully submitted,

Thomas Saporito, Senior Consultant
Saprodani Associates
401 Old Dixie Hwy Unit 3525
Tequesta, Florida 33469
Email: saprodani@gmail.com
Telephone: (561) 972-8363

1 Three Attachments are included in support of this Supplemental 2.206 Petition.

Attachment-One

10 CFR 37.43 General security program requirements.

(a) *Security plan.* (1) Each licensee identified in § 37.41(a) shall develop a written security plan specific to its facilities and operations. The purpose of the security plan is to establish the licensee's overall security strategy to ensure the integrated and effective functioning of the security program required by this subpart. The security plan must, at a minimum:

(i) Describe the measures and strategies used to implement the requirements of this subpart; and

(ii) Identify the security resources, equipment, and technology used to satisfy the requirements of this subpart.

(2) The security plan must be reviewed and approved by the individual with overall responsibility for the security program.

(3) A licensee shall revise its security plan as necessary to ensure the effective implementation of Commission requirements. The licensee shall ensure that:

(i) The revision has been reviewed and approved by the individual with overall responsibility for the security program; and

(ii) The affected individuals are instructed on the revised plan before the changes are implemented.

(4) The licensee shall retain a copy of the current security plan as a record for 3 years after the security plan is no longer required. If any portion of the plan is superseded, the licensee shall retain the superseded material for 3 years after the record is superseded.

(b) *Implementing procedures.* (1) The licensee shall develop and maintain written procedures that document how the requirements of this subpart and the security plan will be met.

(2) The implementing procedures and revisions to these procedures must be approved in writing by the individual with overall responsibility for the security program.

(3) The licensee shall retain a copy of the current procedure as a record for 3 years after the procedure is no longer needed. Superseded portions of the procedure must be retained for 3 years after the record is superseded.

(c) *Training.* (1) Each licensee shall conduct training to ensure that those individuals implementing the security program possess and maintain the knowledge, skills, and abilities to carry out their assigned duties and responsibilities effectively. The training must include instruction in:

(i) The licensee's security program and procedures to secure category 1 or category 2 quantities of radioactive material, and in the purposes and functions of the security measures employed;

(ii) The responsibility to report promptly to the licensee any condition that causes or may cause a violation of Commission requirements;

(iii) The responsibility of the licensee to report promptly to the local law enforcement agency and licensee any actual or attempted theft, sabotage, or diversion of category 1 or category 2 quantities of radioactive material; and

(iv) The appropriate response to security alarms.

(2) In determining those individuals who shall be trained on the security program, the licensee shall consider each individual's assigned activities during authorized use and response to potential situations involving actual or attempted theft, diversion, or sabotage of category 1 or category 2 quantities of radioactive material. The extent of the training must be commensurate with the individual's potential involvement in the security of category 1 or category 2 quantities of radioactive material.

(3) Refresher training must be provided at a frequency not to exceed 12 months and when significant changes have been made to the security program. This training must include:

(i) Review of the training requirements of paragraph (c) of this section and any changes made to the security program since the last training;

(ii) Reports on any relevant security issues, problems, and lessons learned;

(iii) Relevant results of NRC inspections; and

(iv) Relevant results of the licensee's program review and testing and maintenance.

(4) The licensee shall maintain records of the initial and refresher training for 3 years from the date of the training. The training records must include dates of the training, topics covered, a list of licensee personnel in attendance, and related information.

(d) *Protection of information.* (1) Licensees authorized to possess category 1 or category 2 quantities of radioactive material shall limit access to and unauthorized disclosure of their security plan, implementing procedures, and the list of individuals that have been approved for unescorted access.

(2) Efforts to limit access shall include the development, implementation, and maintenance of written policies and procedures for controlling access to, and for proper handling and protection against unauthorized disclosure of, the security plan and implementing procedures.

(3) Before granting an individual access to the security plan or implementing procedures, licensees shall:

(i) Evaluate an individual's need to know the security plan or implementing procedures; and

(ii) If the individual has not been authorized for unescorted access to category 1 or category 2 quantities of radioactive material,

safeguards information, or safeguards information-modified handling, the licensee must complete a background investigation to determine the individual's trustworthiness and reliability. A trustworthiness and reliability determination shall be conducted by the reviewing official and shall include the background investigation elements contained in § 37.25(a)(2) through (a)(7).

(4) Licensees need not subject the following individuals to the background investigation elements for protection of information:

(i) The categories of individuals listed in § 37.29(a)(1) through (13); or

(ii) Security service provider employees, provided written verification that the employee has been determined to be trustworthy and reliable, by the required background investigation in § 37.25(a)(2) through (a)(7), has been provided by the security service provider.

(5) The licensee shall document the basis for concluding that an individual is trustworthy and reliable and should be granted access to the security plan or implementing procedures.

(6) Licensees shall maintain a list of persons currently approved for access to the security plan or implementing procedures. When a licensee determines that a person no longer needs access to the security plan or implementing procedures or no longer meets the access authorization requirements for access to the information, the licensee shall remove the person from the approved list as soon as possible, but no later than 7 working days, and take prompt

measures to ensure that the individual is unable to obtain the security plan or implementing procedures.

(7) When not in use, the licensee shall store its security plan and implementing procedures in a manner to prevent unauthorized access. Information stored in nonremovable electronic form must be password protected.

(8) The licensee shall retain as a record for 3 years after the document is no longer needed:

(i) A copy of the information protection procedures; and

(ii) The list of individuals approved for access to the security plan or implementing procedures.

[78 FR 17014, Mar. 19, 2013; 79 FR 58671, Sept. 30, 2014]

Page Last Reviewed/Updated Friday, October 02, 2015

Attachment-Two

bgr.com

New rifle shoots drones out of the sky without firing a single bullet

Zach Epstein

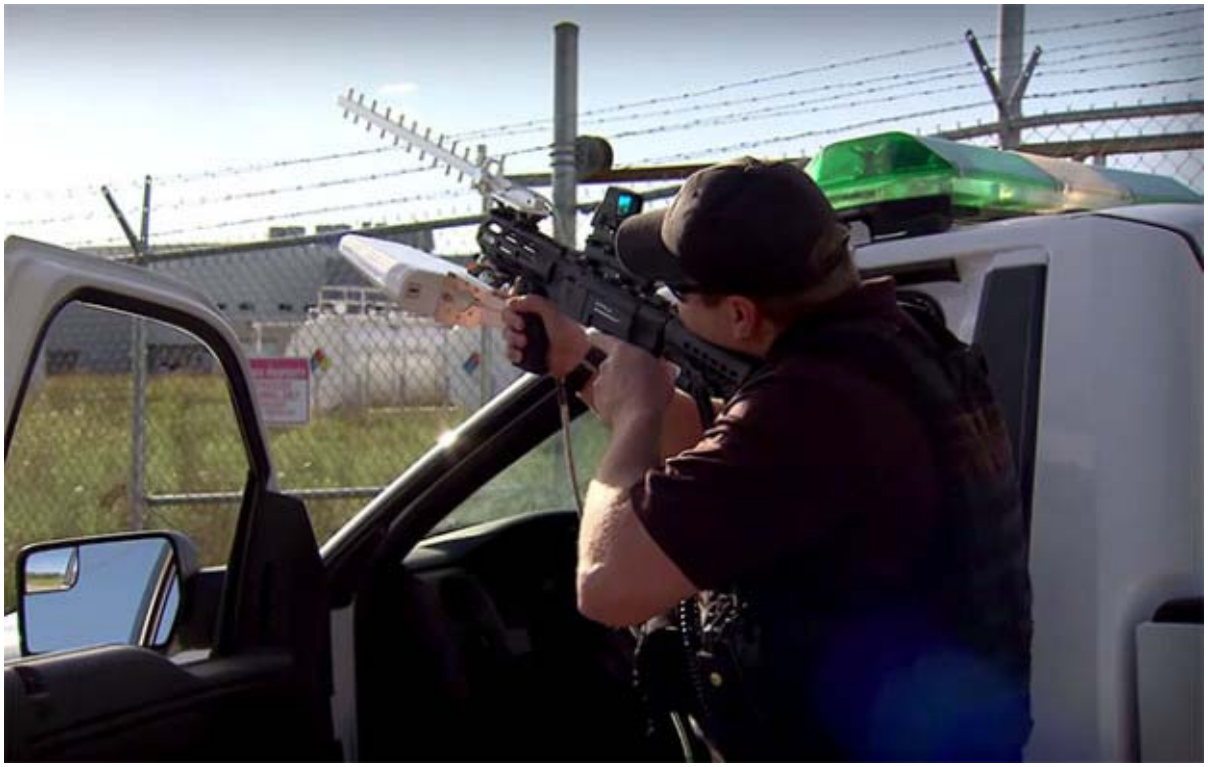
One would need to be quite the marksman to shoot a drone out of the sky with a conventional rifle. Firing a bullet with a diameter of only about 7mm and hitting an airborne drone from several hundred feet away is obviously no easy task. But a new rifle unveiled earlier this week is a game changer for individuals and organizations looking to protect their privacy and safety by warding off snooping drones, and it doesn't even fire a single bullet.

MUST SEE: Adobe confirms major Flash vulnerability, and the only way to protect yourself is to uninstall Flash

Ohio-based nonprofit research and development firm Battelle this week unveiled a device it calls the DroneDefender, which it says is "the first portable, accurate, rapid-to-use counter-weapon to stop suspicious or hostile drones in flight, providing critical security protection at home and abroad." While it's not a weapon in the conventional sense, it represents a huge step in the fight against unwanted drone activity.

There's a fight against unwanted drone activity?

While the term “drone” has recently had its scope extended to include a wide range of simple radio controlled quadcopter aimed at recreational use, not all drones are fun little gadgets. Drones are used regularly as invasive tools intended to spy on individuals or even top-secret business operations. Beyond that, military, governments and law enforcement are targeted by spy drones on reconnaissance missions.



The DroneDefender may be our first look at the perfect anti-drone technology. The device, which looks like a modern rifle with an antenna mechanism attached to the front — because that’s basically what it is — uses targeted radio waves to force drones out of the sky. The nondestructive tech “utilizes a non-kinetic solution to defend airspace up to 400m against UAS, such as quadcopters and hexacopters, without compromising safety or risking collateral damage.”

Regulations in many regions obviously prevent people from firing conventional weapons at drones as a means of defense, so the DroneDefender rifle could be an ideal workaround. The device also has a range of more than 1,300 feet, and that may even improve in future versions.

“This is just the kind of tool we need to safely counter a drone threat,” said Battelle’s lead researcher Dan Stamm. “The DroneDefender can help protect us from those who may wish to do us harm.”

“It can help us in numerous settings, from the White House lawn to bases and embassies overseas; from prisons and schools to historic sites,” technical director Alex Morrow added. “It easily and reliably neutralizes the threat.”

The video embedded below shows a demo of the DroneDefender in

action. While the demo is simulated due to federal regulations in the U.S., Battelle notes that it has been successfully tested in the field numerous times.

Attachment-Three

livescience.com

Signal-Scrambling Tech 'Freezes' Drones in Midair

A new device that can detect, target and deter commercial drones could be used to keep the flying robots away from areas where they're not wanted, like government properties, airports or your own backyard.

The new Anti-UAV Defense System (AUDS) was developed by three tech companies in the United Kingdom. It has a radar detection component, advanced tracking capabilities and a sneaky little onboard device that keeps drones at bay.

Rather than melting drones in midair like Boeing's new Compact Laser Weapons System, AUDS shoots the flying vehicles with something that doesn't destroy them — radio waves. Drone operators typically communicate with, and direct, the aerial bots using radio signals. [5 Surprising Ways Drones Could Be Used in the Future]

Enter AUDS, which uses a drone's communication system against it. Using directional antennas pointed at the drone, AUDS sends the unmanned aerial vehicle (UAV) radio signals that interfere with the radio signals coming from the remote operator. When the drone

picks up AUDS' signals, it "freezes," unsure of where to fly.

Whoever is controlling the anti-drone system can keep the UAV hovering at a distance until the machine runs out of battery life and crashes to the ground, according to a report by the BBC.

AUDS can spot a drone from about 5 miles (8 kilometers) away. After zeroing in on its target, it uses video and thermal imaging software to keep the flying vehicle in its sight. Once the drone gets close enough to the anti-drone system, it's "game over" for the drone.

Drone disturbance

Even though drones can be incredibly useful— they can help conservationists keep tabs on protected areas and help farmers survey their crops more quickly — these flying robots have stirred up quite a few problems in recent months.

Just today (Oct. 9), two people operating a small drone near the Washington Monument in Washington, D.C., accidentally crashed their UAV on the back lawn of the White House. A similar incident occurred at the presidential residence in January. Drones are prohibited from flying in the U.S. capital, but laws and heavy fines don't seem to keep all drones out.

Commercial drones have also been used in attempts to smuggle contraband goods, like cellphones and weapons, into prisons. And camera-toting drones hovering over private homes have been derided as both a security and privacy concern for residents.

The U.S. Federal Aviation Administration (FAA), which sets guidelines for how and where commercial drones can be flown, has ruled that small UAVs cannot be flown within 5 miles of airports and that they must remain below 400 feet (122 meters), where they are unlikely to interfere with piloted aircraft.

But a recent deluge of complaints from pilots, as well as U.S. Forest Service employees who have spotted the flying bots near wildfires, has led the FAA to take further action against rule-breaking drone operators. The FAA signed an agreement this week that will allow it to test technologies that can detect the position of operators who are flying their drones in restricted areas, such as near airports, according to a report by Phys.org.

Though the AUDS system doesn't promise to help locate errant drone operators, it could be used to keep drones away from restricted areas altogether. The radio-jamming technology aboard AUDS doesn't scramble signals from commercial or military aircraft, which use encrypted signals, so it might be safe to use near airports.

The new anti-drone system has been tested in the United Kingdom, the United States and France, according to the BBC. But there's no word yet on when or where this drone-freezing technology could be used in these countries.

Follow Elizabeth Palermo @techEpalermo. Follow Live Science @livescience, Facebook & Google+. Original article on Live Science.