# Global Center for Preparedness and Resilience, Inc. (GCPR) Confidential, Proprietary & Valuable IP not for Distribution

**INTEGRATED AVIATION INFRASTRUCTURE SECURITY PLATFORM**

The Aviation Sector of our National Transportation Infrastructure System is uniquely vulnerable to natural and manmade Aggressor Threat Risks due to highly concentrated physical plant features which include large volumes of highly flammable liquid fuels and dependence on operationally robust and critically precise utilities and digital systems.

It is self-evident that the US Aviation Transportation System is vulnerable to the evolving impact of Aggressor Drone-borne munition, EMP/IEMI and cyber xsecurity threats. The Global Center is focused on providing an ***Integrated Systems Approach*** to Aviation Infrastructure Risks Mitigation which can achieve significantly improved levels of protection for both Civilian and DOD Aviation Operations. Our program incorporates site surveys and sophisticated multi- Dimensional modeling to determine the candidate Airfield’s Vulnerability/Risk profiles, the development of appropriate Risk Mitigation Strategies, and the Engineering and Management of Systems’ Hardening Construction to support a resilient national aviation logistical system.

## High Threat Aviation Infrastructure Risks include:

1. Large volumes of highly flammable Aviation Fuels stored on site
2. ATC & “Ticketing” dark fiber Hardware Com/Data Systems’ vulnerability
3. Air Field and Administrative Services’ Electrical Power Utilities’ vulnerability

Multiple Aggressor and Swarming Drone attack platforms are today capable of delivering kinetic munitions and electronic payloads weighing up to 150 lbs., over extended distances, sufficient to detonate/ignite Aviation Fuel Tank Farms and disable power and communication systems. This program focuses on Aggressor Drone intercept/kill systems and hardening facilities to protect against EMP/IEMI threats.

North Korea’s ICBM-delivered EMP threat to the US National Grid is fully appreciated by DHS et al, but local high value power and communication systems are vulnerable to targeted attacks as a stand-alone as well as combined with a Grid-level attack. Other vulnerable targets include critical public safety, homeland security and national defense installations, public works, medical, industrial, communications and data centers.

Electromagnetic energy creates (‘induces’) energy potential (voltage) in equipment even when it is not plugged in. That energy could very easily exceed tolerances of the components of the equipment – something as low as a 30V inducement could irreparably damage electronics. Additionally, vulnerability of electronic memory components are at risk; should the electronic memory component physically survives the EMP transient overvoltage event, there remains the strong probability that the critical programming codes it contains may be sufficiently corrupted to render the system inoperable.

## Electromagnetic Threat Categories include:

SID Sudden Ionospheric Disturbance

GMS Geomagnetic Storms

CME Coronal Mass Ejections/ “Solar Flares”

EMP/NEMP Electromagnetic Pulse / Nuclear Electromagnetic Pulse HEMP High Altitude Electromagnetic Pulse

IEMI Intentional Electromagnetic Interference

## Electromagnetic Pulse/High Altitude Electromagnetic Pulse Threats:

Electromagnetic Pulse (EMP) or a Coronal Mass Ejection (CME) from our sun produce high powered electromagnetic ‘rays’ that are very damaging to electrical and electronics based equipment. EMPs and CME events are capable of catastrophic levels of destruction.

Electromagnetic Pulses and Geomagnetic Storms can alter Earth's magnetic field, triggering destructive surging currents in power and microelectronic circuits. EMP/GMS can destroy or immobilize power plants, distribution grids, water and wastewater pumps, communications and data centers, machinery, aircraft and vehicles.

On July 9, 1962, the DOD detonated a 1.4-megaton H-bomb over the Pacific at an altitude of 250 miles. Power circuits were shorted out in Oahu, Hawaii, 900 miles away.

The March 9, 1989 "coronal mass ejection" triggered a geomagnetic storm that knocked out power for 6 million people in Canada and the USA for at least nine hours.

## Types of military EMP include:

Nuclear electromagnetic pulse (NEMP), resulting from a nuclear explosion. This is also known as High altitude nuclear EMP (HEMP), which produces a pulse of a much larger amplitude and different characteristics due to interactions with the Earth's magnetic field. NEMP/HEMP from a nuclear detonation can still be higher than 100,000 volts hundreds of miles away.

**IEMI -** Intentional Electromagnetic Interference

EMP events and IEMI attacks onto power and/or communication lines can have huge impact on systems, the effects varying from the very subtle – errors in data streams and microprocessor instruction operation through to system lockups, hard resets and even permanent damage which renders a system beyond repair.

IEMI differs from most other EM threats in that it typically occupies a narrow frequency band, contrasting with other threats such as lightning and HEMP (high-altitude EMP), which are very broadband in nature.

IEMI threats range from “Radi0 Shack” level to Military; low-cost hardware including modified microwave ovens, Radio Frequency guns or EM jammers that can be bought for a few hundred Dollars. While technically unsophisticated, such attacks could easily cause persistent disruption or damage without leaving an evidence of an attack.

A Diehl pulsar is an off-the-shelf “interference source” capable of emitting a 350MHz damped sine wave output and 120kV/m at 1m continuously for 30 minutes; provided with an appropriate antenna, it is capable of disruption or damage at a long distance.

High power military systems include the Boeing CHAMP missile and the Russian-developed RANETS-E, which is capable of a 500MW output and range of 10km.

Mobile attack platforms can vary from trucks with antennae to Drones and Missiles. Additionally, an Aggressor’s IEMI equipment can be extremely stealthy, especially if fixed equipment can be set in proximity to the targeted system – in a building across the street or even an adjoining room, potentially allowing an attack to go unnoticed for a long time, or possibly to not be noticed at all.

This emphasizes a very critical threat characteristic regarding IEMI protection – target access. Access is in terms of distance either from threat to target in radiated systems, or to incoming power and communications cables for injected conducted disturbances.

## Removal/disbursal of Jet Fuel Storage Tank Farms on Airfield Site

Reduction of on-site volume and disbursal of the Airfield’s Aviation Fuel Tank Farm storage and delivery systems will reduce the threat of airborne drone attack as the smaller, distributed targets are of an individually lower value and are more difficult to attack.

* 1. Significant Reduction of On-Site Airfield Tank Farm fuel volumes to minimum “day tank” capacity requirements, replenished by fuel transfer from off-site, multiple secure supply small, redundant Tank Farms and transfer pumping stations; and redundant dedicated airfield fueling pipelines.
  2. Elimination of Fuel Delivery Tankers to Airfield Site reduces Aggressors’ opportunities to bring large vehicle-borne munitions onto Airfield (re: USMC barracks, Beirut Lebanon 23 October 1983, Khobar Towers, Saudi Arabia, 25 June 1996, Alfred P. Murrah Federal Building, Oklahoma City, 19 April, 1995…)

## Hardened Electrical Power Microgrid Systems and Data Centers

* EMP/IEMI - proofing and physical facility security enhancements to Hardened Back-up Micro-Grid electrical power systems and Data Centers

Delta, British Airways, South West Airlines have recently experienced major operational disruptions due to computerized scheduling and ticketing system problems “supposedly not terrorist related”; Atlanta’s Hartsfield-Jackson Airport suffered a major operational fubar event when a back-up power system failed at the regional Air Traffic Control Center (ATC).

The Global Center’s Board of Directors has a working relationship with major US constructors of novel thin-shell reinforced concrete ferrocement structures, buildings, water and petroleum storage tanks. The structural steel rebar grid-work of the ferrocement reinforced concrete construction system, combined with an integrated metallic, carbon-metallic or carbon fiber screening underlayment creates a “Faraday Cage” which protects these buildings’ contents from high field RF environments; the spacing of the electromagnetic permeable conduits acts as a wave-guide and determines what frequency of electromagnetic radiation is rejected, attenuated or passed.

A hardened Faraday Cage achieves the most complete electromagnetic energy facility protection technology available. This specially configured ferrocement reinforced concrete construction system, appropriately modified with close-space screening underlayment(s) provide a materials- efficient and cost-effective means for achieving CME, EMP, HEMP and IEMI threats protection for critical transportation, public safety, homeland security and national defense installations, water, wastewater and power public works, medical, industrial, dark fiber communications systems and data centers infrastructure.

Additionally, this construction technology achieves Very High Level Threat Protection against kinetic munitions and explosives and achieves FEMA 361, ICC-500 & NSSA Standards providing near absolute protection from EF-5 Tornado, Cat 5 Hurricane, Extreme Wind exceeding 250 MPH, Fire, Flooding and Earthquakes.

## Conclusion

An Integrated Aviation Infrastructure Security Platform for the United States is not currently in place, and is absolutely essential for the protection and well-being of our airport systems network, that includes air carrier based, military, general aviation and private sector general aviation fixed wing and rotary wing aircraft and their associated infrastructure.

Secure transportation mobility and logistics for the efficient modal movement of people, goods, resources and information by air, land, sea and space is fundamental to our economic and social well-being.

Air transportation is an essential modal element that must be protected in order to have a resilient system of movement that is safe, secure, healthy and sustainable.

We must be cognizant at all times of threats associated with advanced technology and delivery systems, combined with geo-political entities that may have ulterior motives.