**CODENAME: CONFIDENTIAL**

**MCE123SM TECHNOLOGY DEVELOPMENT**

LAW ENFORCEMENT

SECURITY SYSTEMS

**DRAFT**

9/18/2022 7:46:00 PM

**LAW ENFORCEMENT SECURITY SYSTEMS**

AUTONOMOUS LAW ENFORCEMENT SIMULATION PREVENTION SECURITY SYSTEMS (**2022**) – ensures that audio/visual computer simulations are not used to simulate or investigate or interrogate others about law enforcement, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTONOMOUS LAW ENFORCEMENT SECURITY (**2022**) – makes sure lawsuits are defended remotely, that any protectee of **CRYPTONYM**[:***PATRICK***:] or all protectees of **CRYPTONYM**[:***PATRICK***:] are presentable first, that all criminals are caught, that **MIND CONTROL** stops, that all physical medical conditions have been fully resolved, that all work of all protectees of **CRYPTONYM**[:***PATRICK***:] is completed, that all lawsuits have been paid, that all corrupted officials have been caught and arrested, as well as **WAR CRIMINALS**, that all good things have been done like **WORLD PEACE** and the bucket list, that everyone has come over to apologize in-person, and that no security breaches will occur before coming over, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTONOMOUS INTERNATIONAL LAW ENFORCEMENT SYSTEM (**2010**, **2022**) – this is an international law enforcement system that links with multiple other types of international, multi-national, and national law enforcement systems. The purpose of this system from an international perspective is to ensure that information sharing is safe, while also providing safe information sharing capabilities. This system has systems check mechanism with an International National Security System, and several other systems that pertain to Internal-External checks, International Law Enforcement Agencies, and Global Organizations such as checks on International Business, integrations with an International Intelligence Community, a compliance and standards system through the **INTERNATIONAL INTELLIGENCE COURT SYSTEM** (**IIC**/**S**), **UNITED NATIONS SAFETY** (**UN**/**S**), Diplomatic system, and **GLOBAL SPACE SECURITY SYSTEM** (**GS**/**SS**). There are various levels in this system, including security mechanisms to protect the system, and the system has different access levels that work in the opposite of normal communications, such that authorization must be received through a security check, and the security check must be requested, and there are security mechanisms to protect the system from requests for misuse such that the system has multiple layers of internal protections to prevent extortion and corruption from within, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTOMATED MULTI-NATIONAL LAW ENFORCEMENT SYSTEM (**2010**) – this is a multi-national law enforcement system that pertains to law enforcement that occurs between multiple nations, such as on a case-by-case basis, and cases that change nations. This system has systems check link with the **INTERNATIONAL LAW ENFORCEMENT SYSTEM** (**ILE**/**S**). This system allows intelligence sharing that complies with the International Law Enforcement System, while sharing information through isolated channels, private channels, intelligence community sharing, and other types of protected environments, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTONOMOUS LAW ENFORCEMENT EXTORTION SYSTEM (**2022**) – ensures that law enforcement does not do bad things to any protectee of **CRYPTONYM**[:***PATRICK***:], such as false arrests, false accusations, or otherwise unlawful or targeted activities, such as offensive activities by others due to lawsuits, by researching the backgrounds of each law enforcement agent and prosecuting them for their past mistakes so they are so wound up in defending themselves from lawsuits, such as from the families of victims of executed persons, that they cannot prosecute any protectee of **CRYPTONYM**[:***PATRICK***:], and also to use them for offensive purposes if necessary to prevent crime, terrorism, and warfare, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTONOMOUS THREAT INVESTIGATIVE SECURITY SYSTEMS (**2022**) – ensures that all **THREATS** are properly **INVESTIGATED**, to determine **THE SOURCE**, **THE DESTINATION**, and any **INTERMEDIARIES**, and the usage of any **TECHNOLOGIES** or **SOFTWARE**, who or what **INVENTED THE TECHNOLOGIES**, **INVESTIGATIONS** into **THOSE PARTIES**, **PROSECUTE THOSE PARTIES**, **CONDEMN THOSE PARTIES** in **PUBLIC**, and ensure a determination of how **THE THREATS** were made, conveyed to **WHOM** or **WHAT**, for **WHAT PURPOSE**, **WHY**, **HOW**, and **WHEN**, in addition to **WHO** or **WHOM** knew about **THE THREATS**, for what purpose any protectee of **CRYPTONYM**[:***PATRICK***:] was informed about or made aware of any **THREATS**, **WHY** they were made aware of **THE THREATS**, **HOW** it was important to an action such as **EXTORTION** of **LEGAL RECORDS** to make any protectee of **CRYPTONYM**[:***PATRICK***:] aware of any **THREATS**, how **THE EXTORTION** was used, what **THE EXTORTION** accomplished for **THE DEFENDANT**, what the nature of **THE DEFENDANT**’s business is, and compile **CRIMINAL COMPLAINTS** against **THE DEFENDANT**, automatically, cross-correlate any other **PRIMARY SOURCES** or **SECONDARY SOURCES** pertaining to **THE DEFENDANT**, mark the **DEFENDANT** as a known **CRIMINAL** or **WAR CRIMINAL** or **TREASONOUS PERSON**, whichever applicable, launch **COMPREHENSIVE CRIMINAL INVESTIGATIONS** and **WAR CRIMES INVESTIGATIONS** into **THE DEFENDANT**, **PROSECUTE THE DEFENDANT**.

AUTOMATED VEHICLE LINGUISTICS SATELLITE SURVEILLANCE DETECTION SYSTEM (**2010**, **2022**) – this technology pertains to the use of satellite surveillance to automatically identify patterns of organized cars, such as multiple cars that pertain to organized uses of vehicles that incite threats, and other types of organized uses of vehicles such as multiple organized vehicles with organized national security contingencies, and the linguistics of moving various types of vehicles to various roads and intersections, various timing of vehicle movements, and organizations of vehicle movements to intersect with other vehicles in such patterns, in order to determine how to minimize such occurrences that could exploit and/or extort foreign intelligence through the vehicle movements, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTOMATED VEHICLE LINGUISTIC BACKGROUND CHECK SYSTEM (**2010**, **2022**) – this technology pertains to the system check of **SIGNALS INTELLIGENCE** (**INTELLIGENCE\_CHANNEL**[:***SIGINT***:]) within the **INTELLIGENCE COMMUNITY** (**IC**) to determine if there is a correlation of vehicle linguistic movements to other linguistics, such as organized national security contingencies, organized business activities that are based on extortion through the vehicle movements, organized vehicle movements that are planned for purposes that are unlawful such as attempts to extort law enforcement and/or the military, and a probability check to determine what the correlation would be based on a percentage of the vehicle movement being a direct correlation to a national security contingency threat. This system would be able to build profiles based on the vehicle movements, such as identifying if the vehicle movements are re-occurring, part of a larger organization of vehicle movements, if there has been any communication regarding the vehicle movements with other persons such as uses of telephones, e-mail, and/or visitations with such persons that correlate to multiple vehicle movements that all correlate to national security contingency threats, and also the ability to determine what vehicle(s) and person(s) are being targeted by the linguistic movement of vehicles in the proximity. This technology would be able to build a background and determine if there is a necessity based on the threat type(s) of the linguistic targeting to keep the vehicle(s) away from protected area(s), to dispatch police and/or metropolitan to pull the vehicle linguistics over and/or based on the characteristics of the specific vehicle(s) determine what the best characteristics of the activities would be – such as pulling over the specific vehicle(s) that are conducting the linguistics targeting and where / when to conduct such pulling over of such vehicles, such as determining a dispatch target(s) on a back road based on identified satellite intelligence that was based on selecting the target(s) and monitoring for a date and time that the vehicle(s) violated speeding laws such as +10 to +15 over the speed limit on a back road, such that the targeting is based on identification of multiple violations detected of the linguistic movement of vehicle(s) from satellite surveillance including targeting other vehicle(s) with the background and the speeding that was detected based on the satellite surveillance that was legally established due to the linguistic movement of vehicle(s) having been detected previously, and then the HUMINT based police vehicle dispatch is set to detect a violation by the vehicle(s) such as speeding +10 to +15 over the speed limit, such that if the linguistic movement of vehicle(s) is in violation of other laws then the driver(s) are likely to violate other law(s) such as the speed limit, and the surveillance monitoring is able to monitor rather that put a monitoring responsibility on the police department(s). This type of a system would involve the **FEDERAL BUREAU OF INVESTIGATION** (**FBI**), the **DEPARTMENT OF HOMELAND SECURITY** (**DHS**), the **NATIONAL SECURITY AGENCY** (**NSA**), and the **NATIONAL GEOSPATIAL INTELLIGENCE AGENCY** (**NGIA**) to ensure all the configurations are legal, such that the system needs to be able to ensure that the vehicle(s) that are being targeted by the vehicle movement linguistic(s) are not grouped together with the other vehicle(s), such as undercover, administration, policy workers, and other types of officials are not targeted by the system. There is no ‘guilty by association’ of vehicles in the proximity of a target, such that the target vehicle of third-party vehicle linguistic movements does not establish a legal relationship between the target vehicle and the third-party activities. If there was no organization of the vehicle(s) authorized in the direct communication and/or the direct implied communication, such that the target vehicle(s) reasonably had complete control of the advance planning of the exact vehicle(s) that conducted the linguistic vehicle movement(s), then the target vehicle may have been a target of the linguistic vehicle movement(s) based on third party story creation and/or third party political targeting. If the third party activities have any correlation to psychological data obtained from geospatial psychological satellite surveillance, and there was no intention of the specific vehicle(s) moving in the exact specifics of the data and there was reasonable advance planning of the exact movement(s) verified by multiple forms of planning, then there was no authorization for such movement(s), and issue(s) relating to third parties conducting investigations and/or extortions based on obtaining geospatial psychological satellite surveillance data may indicate a potential third party violation of Constitutional Law, because if there was no specific authorization for the specific vehicle movement(s), such that the vehicle(s) were not authorized vehicle(s), then there was no authorization, and any uses of grid-based vehicle dispatch from a psychological channel must occur with either the requirement of active law enforcement / military law enforcement management and background knowledge, experience, and reasoning that substantiates the use of such abilities – such as active **SPECIAL COMPARTMENTALIZED INTELLIGENCE** (**SCI**) clearance through military intelligence jurisdiction, or an emergency that individual(s) are detected as needing help that absolutely needs law enforcement, **EMERGENCY MEDICAL SERVICES** (**EMS**), and/or fire department attention and the individual(s) are unable to use the phone due to the emergency – and such emergencies may also warrant the utilization of the electronics in phone(s) in proximity to communicate with the individual(s) on an emergency basis, such as the activation of the speaker phone if the phone cannot be physically reached for at the time of the emergency.

AUTOMATED DETECTED VEHICLE LINGUISTICS DISPATCH SYSTEM (**2010**, **2022**) – this system pertains to the actual dispatch selection, and the various potential options for dispatch, such as the use of telephone from the managing agency of the test pilot program to the chief of police of the specific jurisdiction, and/or other types of dispatch such as multi-media conferencing from the dispatch agent of the managing agency of the test pilot program with the chief of police of the specific jurisdiction and a police officer in a police vehicle, and after the testing of the test pilot program the options of various types of electronic dispatch such as requesting the dispatch from the police department of the specific jurisdiction or sending the vehicle directly. This system may include various layers of security, for instance the use of the **FEDERAL BUREAU OF INVESTIGATION** (**FBI**) to protect the **DEPARTMENT OF HOMELAND SECURITY** (**DHS**), the use of **DEPARTMENT OF HOEMLAND SECURITY** (**DHS**) to protect **NATIONAL SECURITY AGENCY** (**NSA**), and the use of the **NATIONAL SECURITY AGENCY** (**NSA**) to protect the police jurisdictions.

AUTOMATED INTERNET TRAFFIC PATTERN LINGUISTICS AND CORRELATIONS ANALYSIS SYSTEM (**2010**, **2022**) – this systems technology pertains to the identification of patterns and linguistics used to access the Internet, and determine what the patterns and linguistics could indicate, and what the indications suggest, in addition to check for correlations to determine if there are correlations to the patterns of internet traffic pattern linguistics to any access of information – such as uses of equipment to gather information about the access of information through the Internet, inadvertent release(s) of information regarding access of information through the Internet, and/or correlations of internet traffic pattern linguistics to other activities, national security, and/or other types of correlations. The purpose of this system is to determine if there are any correlations, and how the correlations may suggest third party violations of privacy, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTOMATED CALLER ID SPOOFING IDENTIFICATION SYSTEM (**2010**, **2022**) – this systems technology pertains to the identification of all callers that use **CALLER ID SPOOFING**, through revealing the actual phone number that was used to place the call. This system also has the capability of determining if the callers have in any way misrepresented the calls such as attempting to use the number of law enforcement as the spoofed **CALLER ID**, such as attempting to target the placed call through the misrepresentation of a law enforcement office. This type of system is important in multi-layered security, because of systems that check the relevance of the call based on known numbers. The **CALLER ID SPOOFING IDENTIFICATION SYSTEM** ensures that security is not compromised through misuses of **CALLER ID**, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTOMATED MULTI-JURISDICTIONAL CONFLICT RESOLUTION SYSTEM (**2010**, **2022**) – this technology pertains to the multi-jurisdictional conflict resolution of political, legal, and other types of conflicts, such that internal-internal and internal-external conflicts are able to be resolved based on the analysis of all of the various parties to the conflict and ensuring that all of the conflict aspects are resolved without negatively affecting any of the parties, and ensuring that all of the parties reach their greatest goals and are placed on the path of their wishes, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

AUTOMATED MULTI-AGENCY SUBPOENA SYSTEM (**2010**, **2022**) – this is a multi-layered Federal, Intelligence Community, Multi-National, and International Subpoena Machine that prevents legal investigations into uses of intelligence sharing, such that the uses of intelligence sharing are secured through the multi-layered use of subpoenas, and the machine automatically creates the multiple layers of subpoenas and security mechanisms on contingency to ensure that the security of the agencies are protected through the security mechanisms.

EVIDENCE PREPARATION SYSTEMS (**2022**) – catalogs evidence correctly for viewing, storing, accessing, and reference, later, however does not allow modification from any party. Allows for clarification of evidence, such as explanations, however. Allows for flagging and categorization, including tabbing evidence in different categories or sections of an evidence book, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

EVIDENCE PREPAREDNESS SYSTEMS (**2022**) – ensures that others have a proper defensive stance regarding all legal and illegal positions that the opposition could take in public, with regards to any evidence that could be manufactured and released in public, including through the usage of **MIND CONTROL SYSTEMS**, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.

EVIDENCE DATABASE SOFTWARE (**2022**) – logs in evidence, including all source data, such as **IDEAINT** transfer, audio streams, and written/typed evidence to prove where it came from, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED, PERMANENTLY DEFINED**, **PEACEFULLY DEFINED**.