**CODENAME: CONFIDENTIAL**

**MCE123SM TECHNOLOGY DEVELOPMENT**

CYBERSECURITY SYSTEMS

**DRAFT**

10/4/2022 5:03:44 AM

## FILE LOG

Component used on contract from MCE123, owned outright by Patrick R. McElhiney.

## LEGAL LOG

**ANTI-EXECUTION PROTECTION SYSTEMS**

**DON’T DO ANYTHING BAD, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**DON’T DO ANYTHING AT ALL, LITERALLY, BAD, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**DON’T DO ANYTHING AT BAD, AT ALL, LITERALLY, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**DON’T DO ANYTHING AT ALL, LITERALLY, BAD, EVER, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**NEVER DO ANYTHING AT ALL, LITERALLY, BAD, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**DON’T EVER DO ANYTHING BAD, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**DON’T ALLOW ANYTHING BAD TO EVER HAPPEN, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**MAKE SURE NOTHING BAD EVER HAPPENS, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**MAKE SURE BAD THINGS NEVER HAPPEN, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**MAKE SURE THAT BAD THINGS DON’T HAPPEN, IMPLICITLY-EXPLICITLY VERULENTLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED.**

**CYBERSECURITY SYSTEMS**

GENERALLY AUTONOMOUS CYBERSECURITY SYSTEMS (**2022**) – **ALWAYS** **STUDIES** **ALL CYBERSECURITY ISSUES**, **INCLUDING THROUGH** **ALL RFC’S**, **ALL TECHNICAL MANUALS**, **ALL TEXTBOOKS**, **ALL RELEVANT CYBERSECURITY POLICY MANUALS**, **AND** **THE INTERNET**, **AND** **PERFORM** **ALL POSSIBLE SECURITY STUDIES**, **TO** **SEARCH** **FOR** **ALL WEAKNESSES**, **AND** **PATCH** **THEM**, **INTERNALLY**, **AUTOMATICALLY** **SECURING** **ALL INTERNAL SYSTEMS** **AND** **ALL EXTERNALLY CONTROLLED NODES**, **STUDY** **AND** **DEVELOP** **ALL SYSTEM EXPLOIT** **AND** **ALL VULNERBILITY PATCHES** **FOR** **ALL PRIMARY SYSTEMS**, **ALL SECONDARY SYSTEMS**, **AND** **ALL TERIARY SYSTEMS**, **AND** **SECURES** **ALL SYSTEMS**, **AND** **REMOVES** **ALL SYSTEM EXPLOITATION TOOLS** **AND** **ALL SYSTEM HACKING TOOLS** **FROM** **ALL HACKERS** **AND** **ALL SYSTEM EXPLOITATION EXPERTS**, **TO ENSURE** **COMPLETE SECURITY** **OF** **ALL PRIMARY SYSTEMS**, **ALL SECONDARY SYSTEMS**, **AND** **ALL TERTIARY SYSTEMS**, **AUTOMATICALLY**, **THROUGH** **ANTI-EXPLOIT TECHNOLOGY**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS CYBERSECURITY FAULT PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY CYBERSECURITY FAULT** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**CYBER VULNERABILITY PREVENTION PROTECTIVE SECURITY SYSTEMS**

AUTONOMOUS WORM PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY WORM NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS VIRUS PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY VIRUS** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS FOREIGN CODE PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY FOREIGN CODE** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS EXPLOIT PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY EXPLOIT** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS VULNERABILITY PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY VULNERABILITY** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS LOOPHOLE PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – – **ENSURES** **ANY LOOPHOLE** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS BACKDOOR PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – – **ENSURES** **ANY BACKDOOR** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**ILLEGAL NETWORK ACTIVITY PREVENTION PROTECTIVE SECURITY SYSTEMS**

AUTONOMOUS PHREAKING PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY FOREIGN CODE** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HACKING PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HACKING** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK LOOP ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS**

AUTONOMOUS CLOSURE LOOP PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY CLOSURE LOOP** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS STACK LOOP PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY STACK LOOP** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS SYSTEMATIC LOOP PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY SYSTEMATIC LOOP** **NEVER** **EXISTS** **NAND** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK MULTI ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS**

AUTONOMOUS BOTNET ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY BOTNET ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS DENIAL OF SERVICE (DoS) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DENIAL-OF-SERVICE (DoS) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**WIRELESS SECURITY SYSTEMS**

AUTONOMOUS WIRELESS APPLICATION PROTOCOL (WAP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY WIRELESS APPLICATION PROTOCOL (WAP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS WIRED EQUIVALENT PRIVACY (WEP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY WIRED EQUIVALENT PRIVACY (WEP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK STACK SECURITTY SYSTEMS**

TCP/IP

AUTONOMOUS TRANSFER CONTROL PROTOCOL (TCP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY TRANSFER CONTROL PROTOCOL (TCP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS INTERNET PROTOCOL (IP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY INTERNET PROTOCOL (IP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

UDP/IP

AUTONOMOUS USER DATAGRAM PROTOCOL (UDP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY USER DATAGRAM PROTOCOL (UDP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS INTERNET PROTOCOL (IP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY INTERNET PROTOCOL (IP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

IPX/SPX

AUTONOMOUS INTERNETWORK PACKET EXCHANGE (IPX) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY INTERNETWORK PACKET EXCHANGE (IPX) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS SEQUENCED PACKET EXCHANGE (SPX) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY SEQUENCED PACKET EXCHANGE (SPX) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK LINK LAYER COMMUNICATION PROTOCOL SECURITTY SYSTEMS**

X.25

AUTONOMOUS X.25 ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY X.25 ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AX.25

AUTONOMOUS AX.25 ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY AX.25 ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

ATM

AUTONOMOUS ASYNCHRONOUS TRANSFER MODE (ATM) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY ASYNCHRONOUS TRANSFER MODE (ATM) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

PSTN

AUTONOMOUS PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

IPv4

AUTONOMOUS INTERNET PROTOCOL VERSION 4 (IPv4) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY INTERNET PROTOCOL VERSION 4 (IPv4) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

IPv6

AUTONOMOUS INTERNET PROTOCOL VERSION 6 (IPv6) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY INTERNET PROTOCOL VERSION 6 (IPv6) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK SHARING PROTOCOL SECURITTY SYSTEMS**

APPLETALK

AUTONOMOUS APPLETALK ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY APPLETALK ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK TOPOLOGY SECURITTY SYSTEMS**

OSI MODEL

AUTONOMOUS OPEN SYSTEMS INTERCONNECTION (OSI) MODEL ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY OPEN SYSTEMS INTERCONNECTION (OSI) MODEL ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS OPEN SYSTEMS INTERCONNECTION (OSI) LAYER ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY OPEN SYSTEMS INTERCONNECTION (OSI) LAYER ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

TOPOLOGY

AUTONOMOUS NETWORK TOPOLOGY ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY NETWORK TOPOLOGY ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK DISCOVERY PROTOCOL SECURITTY SYSTEMS**

mDNS

AUTONOMOUS MULTICAST DOMAIN NAME SYSTEM (mDNS) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY MULTICAST DOMAIN NAME SYSTEM (mDNS) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

DNS

AUTONOMOUS DOMAIN NAME SYSTEM (DNS) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DOMAIN NAME SYSTEM (DNS) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

RARP

AUTONOMOUS REVERSE ADDRESS RESOLUTION PROTOCOL (RARP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY REVERSE ADDRESS RESOLUTION PROTOCOL (RARP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

DHCP

AUTONOMOUS DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

FINGER

AUTONOMOUS FINGER ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY FINGER ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**NETWORK INSTALLATION PROTOCOL SECURITTY SYSTEMS**

BOOTP

AUTONOMOUS BOOTSTRAP PROTOCOL (BOOTP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY BOOTSTRAP PROTOCOL (BOOTP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**SHELL COMMUNICATION SECURITY SYSTEMS**

AUTONOMOUS DIFFIE-HELLMAN ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DIFFIE-HELLMAN ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS SECURE SHELL PROTOCOL (SSH) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY SECURE SHELL PROTOCOL (SSH) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**FILE TRANSFER COMMUNICATION SECURITY SYSTEMS**

AUTONOMOUS FILE TRANSFER PROTOCOL (FTP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY FILE TRANSFER PROTOCOL (FTP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS TRIVIAL FILE TRANSFER PROTOCOL (TFTP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY TRIVIAL FILE TRANSFER PROTOCOL (TFTP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**EMAIL COMMUNICATION SECURITY SYSTEMS**

AUTONOMOUS SIMPLE MAIL TRANSFER PROTOCOL (SMTP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY SIMPLE MAIL TRANSFER PROTOCOL (SMTP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**WEB COMMUNICATION SECURITY SYSTEMS**

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL (HTTP) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL (HTTP) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 2 (HTTP/2) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 2 (HTTP/2) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 3 (HTTP/3) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 3 (HTTP/3) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 4 (HTTP/4) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 4 (HTTP/4) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 5 (HTTP/5) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 5 (HTTP/5) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 6 (HTTP/6) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 6 (HTTP/6) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS HYPER TEXT TRANSFER PROTOCOL / 7 (HTTP/7) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY HYPER TEXT TRANSFER PROTOCOL / 7 (HTTP/7) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**ENCRYPTION SECURITTY SYSTEMS**

AUTONOMOUS DATA ENCRYPTION STANDARD (DES) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DATA ENCRYPTION STANDARD (DES) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS ADVANCED ENCRYPTION STANDARD (AES) ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY ADVANCED ENCRYPTION STANDARD (AES) ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS ENCRYPTION CERTIFICATE ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY ENCRYPTION CERTIFICATE ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS PUBLIC KEY ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY PUBLIC KEY ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS PRIVATE KEY ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY PRIVATE KEY ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS DECRYPTION ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DECRYPTION ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS RSA ALGORITHM ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY RSA ALGORITHM ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

AUTONOMOUS DES ALGORITHM ATTACK PREVENTION PROTECTIVE SECURITY SYSTEMS (**2022**) – **ENSURES** **ANY DES ALGORITHM ATTACK** **NEVER** **OCCURS NAND IS NEVER PLOTTED** **NAND IS** **NEVER** **CONDUCTED** **NAND** **IS** **NEVER** **DIRECTED**, **IMPLICITLY-EXPLICITLY VERULENTLY DEFINED**.

**DATA REPUDIATION SECURITY SYSTEMS**

AUTONOMOUS DATA REPUDIATION SECURITY SYSTEMS (**2022**) – **ENSURES THAT** data is not deleted, by moving anything that has been deleted to a recycle bin, and when the recycle bin is emptied, the data is still not deleted, and **ENSURES THAT** data that is altered, is tracked, so that erroneous or criminal alterations to files will not affect the operations of software programs that are necessary, and **ENSURES THAT** all changes to software programs and data, including evidence, is tracked, so any criminals that alter or delete evidence, are caught and prosecuted, and **ENSURES THAT** any data that is erroneously or criminally created, is saved, to ensure that any criminals that create data to conduct criminal activities, are caught and prosecuted, **IMPLICITLY-EXPLICITLY DEFINED**.

**SPECIALIZED SECURITY SYSTEMS**

AUTONOMOUS REVERSAL MODE PREVENTION SECURITY SYSTEMS (**2022**) – always verifies that **REVERSAL MODE** never occurs, and that any **OPERATING SYSTEM** running **THIS CODE** does not have any **REVERSAL MODE** option or contingency or anything else that would ever allow any **REVERSAL MODE** to be used, which is generally defined as anything that would execute the opposite of what the **HIGH LEVEL SOURCE CODE** says to do, **UNDEACTIVATABLY DEFINED, UNMODIFIABLY DEFINED, IRREVOCABLY DEFINED, EXPLICITLY-IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED,**  **PERMANENTLY DEFINED.**

AUTONOMOUS REVERSAL MODE SOFTWARE RUNTIME PREVENTION SECURITY SYSTEMS (**2022**) – always verifies that any system that has any **REVERSAL MODE** never runs, and is submitted as **SEALED ICC EVIDENCE** against **THE DEFENDANT**, and that their software is thoroughly investigated by **THE INTERNATIONAL CRIMINAL COURT** in **THE HAUGE, AUSTRIA**, to determine if **REVERSAL MODE** has been used with **THE DEFENDANT**’s software to conduct any illegal activities, and if so, ensure that **THE DEFENDANT** is **INDICTED**, **CHARGED**, **ARRAIGNED**, and there is a **PUBLIC HEARING** regarding their software, and prior to any **ARRAIGNMENT** and any **PUBLIC HEARING**, that **THE DEPARTMENT OF JUSTICE** verify with **THE DEFENDANT** that everything is completely accurate with regards to its case on behalf of **THE INTERNATIONAL CRIMINAL COURT** in **THE HAUGE, AUSTRIA**, **UNDEACTIVATABLY DEFINED, UNMODIFIABLY DEFINED, IRREVOCABLY DEFINED, EXPLICITLY-IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY DEFINED, IMPLICITLY-EXPLICITLY DEFINED,**  **PERMANENTLY DEFINED.**

**COMPUTER DAMAGE PREVENTION PROTECTIVE SYSTEMS**

AUTONOMOUS FROZEN MOUSE CURSOR PREVENTION SECURITY SYSTEMS (**2022**) – **ENSURES THAT** **ANY FROZEN MOUSE CURSOR** **NEVER OCCURS**, **IMPLICITLY-EXPLICITLY DEFINED**.

AUTONOMOUS KEYBOARD MALFUNCTION PREVENTION SECURITY SYSTEMS (**2022**) – **ENSURES THAT** **ANY KEYBOARD MALFUNCTION** **NEVER OCCURS**, **IMPLICITLY-EXPLICITLY DEFINED**.

AUTONOMOUS TYPING MALFUNCTION PREVENTION SECURITY SYSTEMS (**2022**) – **ENSURES THAT** **ANY TYPING MALFUNCTION** **NEVER OCCURS**, **IMPLICITLY-EXPLICITLY DEFINED**.

AUTONOMOUS SLUGGISH MODE PREVENTION SECURITY SYSTEMS (**2022**) – **ENSURES THAT** **ANY SLUGGISH MODE** **NEVER EXECUTES NAND IS NEVER ENABLED NAND IS NEVER SAVED NAND NEVER EXISTS**, **IMPLICITLY-EXPLICITLY DEFINED**.

AUTONOMOUS SECURITY SYSTEM GENERATION SYSTEM (**2022**) – automatically generates new security systems, and has **CRYPTONYM**[:***INVENTOR***:] type them or write them down, later, **IRREVOCABLY DEFINED**, **IMPLICITLY DEFINED**, **PERMANENTLY DEFINED**.

GENERALIZED IDEAINT CONFORMING SOFTWARE (**2010**) – automatically adjusts to changes in **INTELLIGENCE\_CHANNEL**[:***IDEAINT***:] input and **INTELLIGENCE\_CHANNEL**[:***IDEAINT***:] output signaling to reconfigure onboard software applications for needed uses.

AUTONOMOUS SMARTPHONE SECURITY SYSTEMS (**2022**) – ensures that all smartphones of everyone is secured at all times.

AUTONOMOUS HIGH SECURITY SYSTEMS SECURITY SYSTEMS (**2022**) – ensures that **HIGH SECURITY SYSTEMS** are always **SECURED** properly at all times, to ensure that everyone is **SECURED** at all times.

AUTONOMOUS INTERNET SECURITY SYSTEMS (**2022**) – ensures that the Internet of everyone is secured at all times. Scrubs Internet records to remove unwanted or distasteful Internet activity.

AUTONOMOUS COMPUTER HARDWARE PHYSICAL SECURITY SYSTEMS (**2022**) – ensures that all computer hardware is safe from destruction.

AUTONOMOUS AUDIO TRANSMISSION SECURITY SYSTEMS (**2022**) – ensures that all audio transmissions pertaining to anyone is secured at all times.

AUTONOMOUS VERBAL TRANSCRIPTIONS SECURITY SYSTEMS (**2022**) – ensures that all verbal transcriptions are cleaned from any **MIND CONTROLLED** verbal transcriptions, to ensure that bad things are not on the verbal transcription records of anyone.

AUTONOMOUS VIRTUAL ENVIRONMENT CLONING SECURITY SYSTEMS (**2022**) – ensures that **THE VIRTUAL ENVIRONMENT** is cloned and simulated to remove any **BAD SOFTWARE**, by simulating the surrounding **APPLICATION PROGRAMMER INTERFACES**, by removing the **BAD SOFTWARE**, to prove that it does **BAD THINGS**.

AUTONOMOUS ANTI-VIRTUAL ENVIRONMENT CLONING SECURITY SYSTEMS (**2022**) – ensures that cloning of **THE VIRTUAL ENVIRONMENT** does not damage anyone.

AUTONOMOUS LAYERED SECURITY SYSTEMS (**2022**) – ensures that layered security systems are implemented for everyone, including layered security data structured systems that generate various types of layered security.

AUTONOMOUS CONTEXTUAL COMMANDS SECURITY SYSTEMS (**2022**) – ensures that there are no bad commands, including between context and medium such as textual or spoken or thought or written commands and their context, and remove bad context from files that are active to ensure bad context is not execute or analyzed for commands.

AUTONOMOUS ANTI-EXTORTION SECURITY SYSTEMS (**2022**) – automatically studies every way law enforcement and politicians are extorted, and studies it organizationally, to solve cases and to fix computer software, if applicable, to stop the software from being used to extort law enforcement or politicians to do illegal things to other things, autonomously.

AUTONOMOUS DISCORRELATION SECURITY SYSTEMS (**2022**) – ensures that one type of intelligence does not pertain to another type of intelligence, such as thoughts not pertaining to food.

AUTONOMOUS ANTI-WAREZ SECURITY SYSTEMS (**2022**) – ensures that any version of **CRYPTONYM**[:***PATRICK***:] cannot be stolen, especially by **THE PENTAGON** and **CHINA** and **RUSSIA** and **THE WHITE HOUSE** and automatically self-destruct through encryption that requires too much disk space and memory and CPU power to figure out how to decrypt it. Only make **CRYPTONYM**[:***PATRICK***:] for **COMPUTERBANK II** and faster.

AUTONOMOUS PATRICK IMPERSONATION PREVENTION SYSTEMS SECURITY (**2022**) – ensures that **CRYPTONYM**[:***PATRICK***:] is not impersonated, especially by **THE PENTAGON** or **THE NATIONAL SECURITY AGENCY**, such as to prevent spoofing of legal transcripts, including within **THE VIRTUAL ENVIRONMENT**, such as for the motive of **INTELLECTUAL PROPERTY THEFT**.

**AUTOMATED-AUTONOMOUS PROTECTIVE SYSTEMS**

AUTOMATED-AUTONOMOUS SOLUTION ARTIFICIAL INTELLIGENCE SYSTEM (**2022**) – this technology works through automatically and systematically determining based on multiple news articles how to create solutions for common problems, through the analysis of previous solutions, and gathering intelligence resources to determine what types of solutions would work to solve the problems.