Communications White Paper
Proposed MonkeyNet

Purpose:

The purpose of this document is to outline, and describe, a Communications System, that can be used by Monkeys, to keep in communications, should the Internet become unavailable, Locally, Regionally, or Nationally. This could be for a variety of reasons, for which are not necessarily predictable, or know at this time.

Basic Messaging:

In any Communications System, at its simplest incarnation, it is two people exchanging information. For this Network, it will be assumed that ALL Communication Messaging will be handled with a SECURE Messaging System, that only Authenticated Users can access, via a number of SECURE Messaging formats. Authenticated in this context means, that the Individual, or Group, originating the Message is KNOWN to, and previously vetted to, the Network. At the conclusion of a successful Vetting Process, the Individual, or Group will receive an Original MonkeyNet Documentation Package which consist of the following:

1. MonkeyNet Documentation and Operations Manual in PDF format.
2. A Windoz XP Application called "OnePad"
3. A Windoz XP Application called "Stego"
4. A Windoz XP Application Suite called "Gnpg4win"
5. A windoz XP Application called "Skype"
6. A set of Original Distribution Generated Matrices, and GPG KeySets.
7. Book Code System, using a commonly held Book. (maybe be "Lights Out" by our own Halffast)

For Groups, this will go to the Groups Comms Guru, and for Individuals, they will get the package. Once the package is received, the User will Generate a Message to either a Master Station or Regional Station using one of the Distribution Matrices, or GPG KeySets, and then they will receive a set of Operational Generated Matrices, and GPG KeySets to use when communicating with the Network. They will be using "The APP" to generate Matrices for local use and to code and decode messages if power is available to run an appropriate computer. If not, then they will be doing all the generation, coding, and decoding, by hand. Instructions for the use of each Specific Messaging System is included in this document under the specific System Headings, as well as in the distribution Documents.

Hardware Layer:

This section describes the possible Hardware used to make Comm Links work. One Time Pad Messaging can be used on ANY unsecured link, while still keeping the Message SECURE. So let us look at the local BASIC incarnation, of how the system works.
You are the Comms Guru for your group, and you need to be able to communicate, Securely, between members of your group, as they may be spread out over ranges farther than can be handled by yelling across the room. You have "The App" and have generated a Symbolic Pad, printed copies of it, plasticized those against the weather, and distributed those to each of the Families, and Individuals in your group. These will have spaces to put in Row/Column Numerics along the top and side of the Matrix, and the Depth, if used, will be decoded by sight, using the Message Key that is transmitted before Message Body. It doesn't matter what the Hardware used in the transmission or reception is, (CB, FRS, GMRS, Paper, or Voice, as the ONLY Item Needed to to make this work SECURELY is the PAD, (Matrix) and the Message Key, the rest can be handled by hand if needs be. The ONLY part of the WHOLE Network, that needs to have PHYSICAL Security, is the Generated PADs, and the GPG KeySets, themselves. Everything else can be in the Public Domain, and it does NOT compromise the Security of the Messaging System. Should a Generated PAD, be lost or compromised, a New one can be generated, either by hand, or by using "The App" and the compromised one discarded. GPG KeySets can also be generated by using the Open Source GPG Encryption Software, referenced in that section of this document. Nothing in this

Network precludes any Authenticated User or Group from establishing a Private SECURE Messaging setup with locally generated PADs, and, or, GPG KeySets, between TWO Groups, or Individuals, as they mutually agree. They will be responsible for the Security of any locally generated PADs, and or KeySets.

Station System:

Regional Comms will be handled by our Monkey Hams that sign up to participate in the MonkeyNet. They will have the capability to use both Short and Long Distance Comms Hardware, to facilitate SECURE Messaging between Groups that are farther apart than can be reached with local AoO Comms Links. They will be responsible for the following:

1. They will generate PADs and GPG KeySets for their Regional Comms Users to use between themselves, and their Regional Users.
2. They will replace any compromised Regional PADs or KeySets and distribute them as required.
3. They will have the capability send OneWay Transmissions by voice, of SECURED Messages, to authenticated Groups or Individuals that have Receive Only capability. (similar to what the WWII British used to communicate with Resistance Groups in Occupied Europe) This will include the capability to send Specific Generated Pads for use by traveling Groups and Individuals, so they can setup local Comms, and FaceMeets, as mutually agreed upon, with specific local Fixed Groups in their line of travel.
4. They will communicate with Master Stations using PADs, and KeySets, generated by Master Stations, and pass general traffic, up the Network, and receive general traffic for their Region, and pass that traffic, down the Network, to authenticated Groups and Individuals in their Region.
5. Should a Regional Station be compromised. The Master Stations will use a pre-generated Master PAD, that only each individual Regional Station has, to warn them, of the compromise, and to destroy all PADs and KeySets from compromised Regional Station. After that is done, Regional Stations will name a New Regional Station, to replace the compromised one. That New Regional Station will then generate a new set of PADs, and GPG KeySets, and pass those to the other Regional Stations and Master Stations, using his UN-COMPROMISED PAD previously used in the Network. Once that is done, the Regional Station can function in the network, as a Regional Station, and generate NEW PADs, and KeySets, and distribute them to the Groups, and Individuals, in that region.

6 Once a Station has been compromised, they will NOT be allowed back into the Network, without Re-Authentication, by a FaceMeet, with either, a Founder, or another Master, or Regional Station. Then only by a unanimous vote of those Stations, will they be authenticated, and only as an Individual Station, and they will not be given any PADs, or KeySets, common to another Group, or Individual, except by Mutual Consent, between the two Parties. They will have only Comms with their local Regional Station, as far as the Network is concerned, and their traffic will be suspect, for a considerable time forward.

7. ANY use of compromised PADs, and KeySets after they are Known to be compromised, will be grounds for dropping that Station, Group, or Individual from the Network. There will be NO EXCEPTION to this rule.

Master Stations will be decided on by the Operators of Regional Stations. Typically they will be located as far out away from populations, and in as inaccessible of locations as possible. There will a Minimum of TWO Master Stations, in the Network. These stations will be the major HUB, for the Network, and will be responsible for the following:

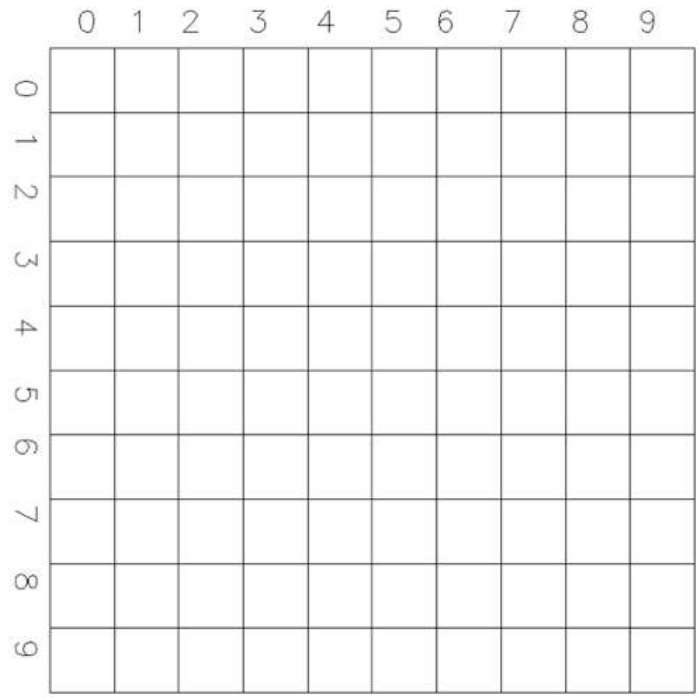
1. They will generate, and store the PADs, and GPG KeySets for ALL comms between themselves, and Regional Stations, as well as PADs and KeySets for direct Comms with Groups and Individuals, should a Regional Station be compromised.
2. They will replace any compromised Regional PADs or KeySets and distribute them

as required.

3. They will have the capability send OneWay Transmissions by voice, of SECURED Messages, to authenticated Groups or Individuals that have Receive Only capability. This will be used as a Backup, for the Broadcasts made by Regional Stations, or as warning that a Regional, Master Station, Group, or Individual, has been compromised.
4. They will be the Central Hub, for traffic, that can not be sent directly between any other authenticated Stations, Groups, or Individuals.
5. Should a Master Station be compromised. The other Master Station will use a pre-generated Master PAD, that only that Master Station has, and distributes to the Regional Stations, separately, to warn them, of the compromise, and to destroy all PADs and KeySets from compromised Master Station. After that is done, Regional Stations will name a New Master Station, to replace the compromised one. That NEW Master Station will then generate a new set of PADs, and GPG KeySets, and pass those to his Regional Stations or if he was a Regional Station to the other Regional Stations, and Master Stations, using his UN-COMPROMISED PADS, previously used in the Network. Once that is done, the New Master Station can function in the network, as a Master Station.
6 Once a Station has been compromised, they will NOT be allowed back into the Network, without Re-Authentication, by a FaceMeet, with either a Founder, or another Master, or Regional Station. Then only by a unanimous vote of those Stations, will they be authenticated, and only as an Individual Station, and they will not be given any PADs, or KeySets, common to another Group, or Individual, except by Mutual Consent, between the two Parties. They will have only Comms with their local Regional Station, as far as the Network is concerned, and their traffic will be suspect, for a considerable time forward.
7. ANY use of compromised PADs, and KeySets after they are Known to be compromised, will be grounds for dropping that Station, Group, or Individual from the Network. There will be NO EXCEPTION to this rule.

One Time Pad Encryption System:

One Time Pads are the MOST Secure form of encryption available to the Regular Joe's, that make up the our intended User Group. In it's simplest incarnation it consists on a Matrix with 10 Rows, of 10 Columns, of Boxes, with each Box given a Row and Column Address, like the following:



Now you can put anything in each Box, and reference it, by just sending the Row/Column Address, in the Encoded Message, and the User on the other end of the link, just needs to lookup the Row/Column Address, using the SAME Matrix, to retrieve the contents of the Box. In the MonkeyNet system, we will be using three types of Matrices.

1. The ASCII Matrix: Where ALL the ASCII Letters, Numbers, and Punctuation, are used to fill the Boxes.
2. The Hexadecimal Matrix: Where ALL the Hexadecimal Characters (0-9 and A-F) are used to fill the Boxes. Multiple instances of each of each character are used until all 100 Boxes are filled. This make Cracking the Matrix by looking at the Message, near Impossible, even for the Big Boys. (NSA)
3. The Symbolic Matrix: Where Each Box contains a Word or Phrase that would be used in a Message. This can be very easy to use for local Secure Comms where Locations, Crossroads, Actions, and other relevant Data, can be sent Securely with speed, and easy to manually decode on the fly.

Examples of each type of simple PADs are shown, along with a typical coded Message, and decoded Text, are in Appendix A.

These simple two Dimensional Matrices will work very well for Local AoO SECURE Messaging over unSecure comm Links. They can be printed out and Plasticized for Weather Protection, and used Manually in the field, especially when a Symbolic Pad is used. All that is required is that both Parties use the Same EXACT Pad. Pad ID Designation will be the Message Key, and consist of an (M) followed by 00-99.
For a Voice Link one would say, "Mike Twenty Two" for the Pad designated #22, at the beginning of the Message.

For the One Time Pad System for use between Master Stations, and Regional Stations, to Groups and Individuals, there is a further Message Key Encryption that will added at the beginning of each Message that will do the following:

1. MessageKeys will be Generated, and Encrypted by a Special Message Key

One Time Symbolic Pad. This Pad will include Numeric Characters 0-9, and include the following, set of symbols. ^, <, >, v, A, H, S. This set of characters will randomized, with multiple Instances, until the 100 Position Pad is full, with the Standard Row/Column addressing, starting with 0 Row and 0 Column in the Upper, AND Lefthand Position.

2. A MessageKey will have the following format. (a) and (b) make up the Pad ID.
   a. Pad ID Type. ASCII, Hex, or Symbol A, H, S,
   b. Pad Number. 01-99
   c. Starting Row Number. 0-9
   d. Ascending or Descending. ^ - v
   e. Starting Column Number. 0-9
   f. Right or Left Order. >, <.

Once the MessageKey is Decoded the Recipient, use the MessageKey to select the appropriate Pre-generated Pad, by it's Pad ID. Place the Number in (c.) in the Upper Left hand Row Box, and then depending on the character in the (d.) above, increment Down one box for the next Number in sequence, or if UP then go to the Bottom of that Row Address column and increment UP, with each Number in Sequence. A similar process will be used to set the Column Address. Place the Number in (e,) in Left most Column, and then depending on the character in (f.) Increment to the RIGHT one Box for the next Number in Sequence, or if Left, then go to the far right Box with the next Number, and increment LEFT with each Number in Sequence.

Examples of this Special MessageKey PAD, and a typical coded MessageKey and decoded MessageKey, are in Appendix B.

This then will be the Basic Format of the MonkeyNet Secure Messaging System. It can be used without any computer, or electrical power, by manually transcribing the the Input Text, or Symbolic Phrases into a Numeric Row Column Address, with a Pad ID. Master Stations, and Regional Stations will presumably have computers, and power, to run the Required Radio Systems, so they will be using, the much more complicated Special MessageKey Pad System, for their comms, but if required, they can use the System, Manually, as well, with just a bit of work. There is a Computer Program called "The APP" that will be distributed with the Original Distribution, that automates much of the above work. It is described in the "The APP" Section of this document.

Multiple Dimension One Time Pad Encryption System:

This is an Extension to the One Time Pad System that will be employed for use in the MonkeyNet System. Mainly for use with "OnePad" but can be used Manually should a User need the added Security or required more than 100 Boxes provided by the Two Dimension system outlined above. What we have done is basically stacked Multiple Pads and added a Numeric Character to the end of the MessageKey, which will be a 2, 3, or 4. No character in this place will denote a single Level PAD.

In the normal Two Dimension system each box is addressed with Row/Column Address. In the Multiple Dimension system we use this Stacked PAD, and start the coding using Level 1 for the first Character, or Symbol Phrase, and then got to the next Level for the second Character or Symbol Phrase, and so on until we reach the Number in the MessageKey, at which time we then go back to Level 1, for the next Character or Symbol Phrase, and repeat until finished coding the message. This greatly complicates any Cracking attempt, and allows any single PAD to be reused many times without worrying about Brute Force Cracking, of the Encrypted Message.

GPG Encryption System:

The GPG Encryption System is based on the original GPG Public/Private Key Encryption System, developed back in the 90's, by Phil Zimmermann. http://en.wikipedia.org/wiki/Pretty_Good_PrivacyBook Code The Open Source version that the MonkeyNet will use

is called the GPG Encryption System, and is based OUTSIDE the USA, so that it does NOT FALL under any US Export Statutes, or US Jurisdiction. It is "Open Sourced" which means the Code, that is used in the Algorithms, and Processes, is available to ANYONE, and ANYONE can see how it works, and more importantly, ANYONE can see that there are NO BackDoors into the Encryption System. No NSA Hanky-Panky in this program. This System, and Programs, can be run on just about ANY OS, and can be downloaded from http://www.gnupg.org. Distribution GPG KeySets will be distributed with the Original Distribution, and when a User sends a GPG encrypted Message to his Regional Station, or a Master Station, they will get in return, a set of Operational KeySets, that, that Specific User, or Group, will use, to communicate with. If a KeySet is compromised, a New KeySet can be generated locally, and distributed to those who need it, using the One Time Pad Encryption System, and notifications can be sent, throughout the MonkeyNet, to delete, the compromised KeySet, along with that KeySet Update Distribution. System and Program Documentation can be obtained from the two URLs listed above.

In the MonkeyNet System, we distribute a complete KeySet, both Public and Private. Regional and Master Stations, would have the complete KeySets, but would distribute just Public Keys to Group, or Individual, Stations.

If you choose to send a message to the whole Network, you have two choices.

1. You can encrypt the Message with the Private Key, and then ANYONE with the Public Key can decrypt it.
2. You can encrypt the message with the Public Key, and ANYONE with the Private Key can Decrypt it.

This means that if you want to make a general Network-wide announcement, you could use Method 1, and ANYONE with that Operational Public Key can decrypt it, OR, if you use Method 2, then only Stations with the Private Key can decrypt the message. I plan on using Method 1 for general MonkeyNet Announcements, from Regional, or Master Stations, to ALL other Stations. Groups and Individuals, would use Method 2, to send messages to Regional and Master Stations, and other Group, or Individual Stations, would not have access to those Messages, that are not directed, specifically, to them, but ANY Regional or Master Station, can decrypt, and answer, as required using a Direct Station to Station KeySet for that Originating Station.

Since the only thing that needs to be held CLOSE, is the Generated PADs, and the GPG KeySets, we will be distributing the Distribution CD, and that can go to anyone, without compromising the SECURITY of the MonkeyNet. Distribution KeySets will NOT be used for Messaging, except to SEND an Authentication Request to the MonkeyNet, for inclusion as a Station or Member. Then the Network Stations will decide, if they can be included, and which Station will be their contact into the MonkeyNet. If approved, than that Station will reply with a Message that includes Operational PADs, and GPG KeySets to that New Station or User. This can all be done on the forum, IF we have the Internet, and if NOT then it can be done with any Comm Link available, even One-way Broadcasts, if need be.

The normal routine for GPG Encryption usage would be for UserA to Publish his Public Key to a Public KeyServer, and others could go there and pick up each of the Public Keys, for the folks they want to send Messages to. Then when someone wants to send a message to UserA they would encrypt the message with his Public Key, and then only UserA can decrypt the message, because only HE has the Private Key, that will decrypt the message. This works wonderful for One to One Messages, but is terrible for One to Many Messages, as there is no way to send a message to more than one User at a time.

OnePad:

Creation of "OnePad" was taken on by the Development Team, to make using the system easier, for those who have power, and a computer, to work with.

The Distribution CD includes an Installer, that can bring a clean Windows XP installation, to be completely updated, with the appropriate SP3, and .Net Framework4, Updates. This allows "The APP" when installed, to RUN, with no further Updates from Microsoft, required.

"OnePad" has a Special Security Provision in it called the "NUKE Button"

This is a Security Provision, REQUIRES that "The APP" when loaded onto a HardDrive, with all its Supporting Files, be in ONE Single, and Separate Folder, from anything else. This Requirement is due to, If the NUKE Button is selected, OnePad asks you one time if you are sure, if you click YES, the application begins overwriting everything that is in the Folder that it resides in, on the computer, multiple times, and then deletes each file, and then the folder itself. It can wipe 2 GB of data in about 15 seconds. This provision can protect all Generated Pads, and GPG KeySets, that are used by "One Pad" and GPG for EnCrypting and DeCrypting Messages, from compromise, should the computer be about to fall into unauthorized hands.

A second Failsafe Provision, is that Users, MUST, use the specific "EraseMonkeyNet.exe" File to launch "OnePad" Should someone just Double Click on "OnePad", or a shortcut, "OnePad" will launch in Security Breach Mode, which shows nothing on the screen, but NUKES the entire Folder, where "OnePad" resides, including all Generated Pads, and GPG KeySets. This FailSafe Provision, when implemented, we hope, will provide Security for the MonkeyNet System, should a computer be Lost, or Compromised, by an OpForce, in a Takeover Senerio. The OnePad Folder can NOT be reloaded until the UnNUKE.exe is run on that hard drive. all Master and Regional Stations will have the UnNUKE,exe file, should you need it. Just a NOTE, here: Just about ALL the Beta Test Group have accidentally, or on purpose, tested out the NUKE Options in one way or another, so don't feel to bad if you find yourself in that situation. We ALL have preceded you, down that road.

"OnePad" will do the following functions, as envisioned by the Development Team.

1. Generate, Edit, Store, Load, and Print, Pads in all four Pad Types, (Ascii, Hex, Symbolic, and Special MessageKey) in from one, and up to four, Dimensional Depths.
2. EnCode, and DeCode Text, and File Messages using any PreGenerated and Stored Pads in the simple, Fixed Row/Column Addressing System.
3. Generate a MessageKey used to EnCode, Text, File, and GPG KeySets, and DeCode those received Messages, when the appropriate Message Key has been loaded into "The APP"
4. Encode and DeCode Text, Files, and GPG KeySets using PreGenerated and Stored GPG KeySets.

Installation:

Installation program will automatically install XP SP3, if missing
Installation program will automatically install MS Framework 3.5 SP1, if missing.

The installer has been tested on and functions correctly on:

Windows XP SP2 (automatically installs ServicePack 3)
Windows XP SP3 32Bit
Windows Vista RTM, SP 1, SP2 (32Bit&64Bit)
Windows 7 RTM, SP1 (32Bit & 64Bit)
Windows Server 2008 R2 Service Pack 1 (64Bit)

The application OnePad has been tested and run on:

Windows XP SP3 32Bit
Windows Vista RTM, SP 1, SP2 (32Bit&64Bit)
Windows 7 RTM, SP1 (32Bit & 64Bit)
Windows Server 2008 R2 Service Pack 1 (64Bit)

Minimum System Requirements:

Windows XP SP3
MS Framework 3.5 Service Pack1
256 Mb Ram
64 Mb Disc space available for extras, pads and keys
400 Mhz Processor

Suggested lSystem Requirements:

Windows XP SP3 or above
MS Framework 3.5 SP1
256+ Mb Ram or more
96 Mb Disc Space for extras, multiple pads (AO, District, Regional, etc) & keys
1 Ghz processor or above.

If you run some other OS, on your computer, (Linux, Mac OSX, or whatever) all the Apps that are part of MonkeyNet, have been tested, and operated, using VirtualBox VMs running any of the above mentioned windows OS's as guest VMs.

Stego: http://en.wikipedia.org/wiki/Steganography

Stego is a Steganography Application, This Stego Application can embed hidden information into the following image types .BMP, .TIF, .PNG... (Pictures) Using Stego to send Operational Pads, and GPG KeySets, make their distribution, Secure without using either "OnePad" or GPG, and gives the MonkeyNet a third Secure Messaging system. Because of the large files required to be transfer in typical Jpeg Stego Files, it will much more useful while there are Wide Bandwidth Comm Links (Internet) still available. The beauty of using this format, to send SECURE Communications, is the information LOOKS Like a picture of GrandMa, or Scenery, or other, than what it REALLY is, An Encrypted Message. Like Hiding in Plain Sight. This version in the Distribution File, is still now in Beta 1.0 another NOTE, here: It has been found that Stego has an issue with saving the Encrypted image in any format other than .PNG. Until we get this limitation fixed, use the .PNG format for any Stego File Outputs used for MonkeyNet.

Skype:

Skype is a Communications Application, now owned by Microsoft, that features Chat, Voice, File Transfer, and Video, communications, World Wide, for Free. It is a basic VoIP Program, with video capabilities that costs the User Nothing, as long as it is used computer to computer. You can ADD, a Phone Line to your Account that will provide a Telco Number that can accept incoming Calls, from the Switched Telephone Network, and from which you may place calls to the Switched Telephone Network. It is a Low bandwidth application when used in Chat Mode, and medium bandwidth application in straight Voice Mode. When in Video Mode it is a High bandwidth Application. We included it in the MonkeyNet system, because it also can transfer Files, simultaneously, with Chat, Audio, or Video connections. This gives the MonkeyNet a broad Internet Footprint, with multiple types, and protocols, of comm Links to chose from, in keeping the communications between Monkeys flowing. Skype would be an Internet Only type Link, and not useful if the Internet is NOT available.

Radio Systems:

For this discussion we are assuming that the FCC Rules and Regulations are still Operational and apply to all Radio Communications, for the MonkeyNet System. Station Identifications, and Callsigns, are only REQUIRED in the GMRS and HAM Radio Sections, but NOT in the CB or FRS Radio Sections, so, Identification of those Sections, will be up to the Users.

Local AoO: (Area of Operations)

1. iDen/ISM SECURE Phones:
   This Comms System is not subject to Scanning, or DF'ing, (Direction Finding) that normal Comms Systems are vulnerable to, and for this reason they are the Comm system of choice for use in local AoO Comms.
   The MonkeyNet Setup on DirecTalk, will be on Channel 5, Spreading Code 5 for those Comms that are undertaken in the Blind. Users can switch, to ANY Mutually Agreeable Comms

Setup. ANY Mutually Agreeable setup can be pre-negotiated between Users, Once local Comms, has been established. For OpSec, it would be advisable to use some other setup for local Squad Comms, than the MonkeyNet Setup, and keep that for Comms with Groups or Individuals outside the local Group. Since these Units are Digital/Spread Spectrum based Comms, they are Secure enough in most circumstances for direct voice use. Where first time FaceMeets are involved, OpSec should require a pre-negotiated, verbal Symbolic Pad Message, to make initial contact, on the MonkeyNet Setup, and then use that verbal Symbolic Pad to negotiate a different setup, for the actual FaceMeet, from either the MonkeyNet setup, or either of the two Parties, Individual Squad Comms setups.

2. CB/FRS/GMRS:
   Since these are essentially Unsecured Comms, and subject to both Scanning and , (DF) basic OPSec needs to be observed. Since these are also basically only local AoO Comms, scanning of these Radio Systems, is a very good way to keep track of just who is in your local AoO, and what they are up to. DF'ing is mostly to complicated, and equipment intensive, to be used by most Users, so we will not be dealing with that subject, here.
   OpSec for Unsecured Comms means basically you do NOT Transmit, messages in the clear, unless absolutely necessary, and if you must you keep those transmissions short, and impart as little information as possible, to get the message across, without giving any Listeners, more information, than is absolutely necessary, to move the critical information between the Units involved.
   MonkeyNet Setup on CB and GMRS/FRS will be on the following Frequencies:

CB.	Channel 5, (27.015 Mhz) and LSB (Lower Sideband) if using a SSB Radio.
FRS	Channel 5S, (462.6625 Mhz) for Interoperation with GMRS Radios.
GMRS	Channel 5S, (462.6625 Mhz) for Interoperation with FRS Radios, using Max of 5 Watts of Tx Power.
	Channel 5 (462.500 Simplex or 462.500T/467.500R Mhz if Duplex) for standard GMRS operation, using a Max of 50 Watts of Tx Power.

   All MonkeyNet Comms should be by Secure Messaging, using verbal Symbolic OneTime Pads. Your Group Squad Comm setup should NOT be on the MonkeyNet Channel. Leave the MonkeyNet Channel free, for use in establishing Comms, with outside Groups or individuals. If you are establishing Comms, outside your Group, then once Comms are established, you should move your Comms to another CB/FRS/GMRS Channel, Preferably NOT your local Squad Comms Channel, for the actually Traffic Handling, or Messaging.

3. Ham: All MonkeyNet Comms will be established by FCC Callsigns , as long as the FCC Rules remain in force. Once that is no longer the case, then Identification of those Sections, will be up to the Users.
   Again, here we are dealing with basic Unsecured Comms, but there is much more bandwidth to select a Operating Frequency from. Local AoO Comms can take place on ANY of the VHF/UHF Ham Bands, and a MonkeyNet Calling Frequency is established for each Band.

10 Meters	28.425 Mhz Am/Fm/Usb/Data (Upper SideBand)
6 Meters	50.150 Mhz Am/Fm/Usb/Data (Upper SideBand)
2 Meters	144.150 Mhz Am/Fm/Usb/Data (Upper SideBand)
1.25 Meters	222.450 Mhz Am/Fm/Usb/Data (Upper SideBand)
70 CMeters	440.500 Mhz Am/Fm/Usb/Data (Upper SideBand)

   MonkeyNet Comms will be by verbal Symbolic OneTime Pads. Nothing precludes individual Users, and Stations, from having unsecured Comms between themselves as they mutually agree upon, with the Understanding, that NO Operational Pads or KeySets, EVER get distributed over UnSecured Comm Links, PERIOD. Violation of this Policy will cause the offender to be Dropped, PERMANENTLY, from the MonkeyNet.

Regional AoO

Regional Comms Frequency, and Emission Standards will be setup by each Regional Station, as required to interoperate with Group and Individual Stations, with which they communicate. Both One Time Pad, and GPG, Encryption Systems, can be used for

Secured Messaging. It assumed that after the Internet ceases to operate, that most Messaging traffic between the Regional Stations, and Master Stations will take place using one of the Digital Emissions. (RTTY, Amtor, PSK, etc) Messaging traffic between Regional Stations and Group or Individual Stations will be by whatever emissions are mutually agreed upon, including Oneway Voice Broadcasts, to those, who have Receive Only capabilities.

MonkeyNet Master Station AoO

Master Stations will be designated, by consensus, of ALL the Regional Stations, with Frequency and Emission Standards developed, in conjunction with the Regional Stations, as required.

Appendix A: Sample Symbolic PAD #01

	0	1	2	3	4	5	6	7	8	9
0	Gallon	P	Cross Roads	I	Up	G	7	Cell Phone	A	House
1	308	1	FRS/ GMRS	8	Pint	T	Barter	P	Mile	Z
2	Right	J	Quart	H	2	Sell	iDen/ ISM Phone	4	Meet-Up	Outside
3	Case	N	S	223	Y	Bridge	E	9mm	Space	F
4	7	Liter	Pallet	Left	I	Km	Code	E	Buy	R
5	4	Kg	U	2	Box	Cabin	D	V	Oz	6
6	Known	U	45ACP	3	9	Period	Face Meet	0	Exchange	M
7	comma	Ton	?	Channel	9	Lbs	CB	5	3	W
8	762X39	B	X	5	O	Ham	L	30-06	6	OpForce
9	1	K	Down	C	30-30	8	Q	A	Gram	Group

Above is a sample of a Symbolic Pad, designed for use by a Local Group, to use over an unSECURED Voice Radio Radio Link. This can be printed and Plasticized, and then distributed to the local Group Members for use. One would then code the following Message, between two Group Members, concerning a Face Meet, with a Know outside Group, for the purpose to Bartering, and or exchanging specific supplies. The Text Message is as follows.

I want you to FaceMeet, with Group Y, who are a known Outside Group. Comms will be via iDen/ISM Phones Channel 8 Code 12. We are looking for 100 Box 308, 50 Box 9mm and we will exchange for 50 USG Diesel 2. Exchange will be 5 miles left of the Crossroads, by the Old Cabin. Meet Up with our Group after, 16 miles down from Bridge. Comms CB Channel 16.

Coded Message will look like this:

S01 44 79 97 31 15 52 66 99 34 60 29 99 38 26 73 95 46 90 53 38 48 11 84 67
54 10 38 48 77 84 81 82 37 38 16 84 67 00 56 32 86 24 70 68 77 18 43 02
67 86 56 55 65 28 67 61 49 99 97 39 15 38 11 88 18 92 35 65 76 73 90 88

Decoded Message Reads:

Pad S01 I want U Face Meet Group Y Known Outside Group _ Comms iDen/ISM Phone Channel 8 Code 12 Buy 100 Box 308 50 Box 9mm_ Barter 50 USG DSL 2, Exchange 5 Miles left Crossroads old cabin. Meet Up our Group aft_16 miles down Bridge. CB Channel 16

Pads can be setup for local use with local names places, and references. The Member doing the Face Meet knows that he only has to get within range of the iDen/ISM Phone for contact, from cover, and then make a decision, if he wants to go thru with the meet. He knows that these folks are a Known Outside Group, with which his group has done business before, and which Group it is. He also knows what his group Needs, and what they have to trade. He also knows that his Group is waiting for word, at a specific location, and has preset Comms on CB Channel 16.

Appendix B: Sample Special Message Key PAD #01

	0	1	2	3	4	5	6	7	8	9
0	A	7	^	8	4	S	1	v	3	9
1	2	0	7	6	8	H	^	8	S	5
2	4	A	^	1	>	H	4	<	6	8
3	H	2	>	7	2	S	<	3	A	3
4	0	>	6	3	H	9	5	1	9	0
5	9	S	<	0	6	5	<	2	6	v
6	a	5	3	7	5	H	^	6	9	v
7	6	0	0	v	0	1	7	2	4	A
8	4	>	H	2	8	S	<	0	8	4
9	v	1	S	3	^	5	1	7	>	A

The above Special MessageKey PAD is a sample of the Pad that will be used to send the Message Key for the Master and Regional Stations, that tells the Receiving Station, the following information.

1. The Pad Type and Number. (Pad ID)
2. How to setup Row, and Column Addressing for this Message.
3. Level Number or Depth Number. No Character is assumed to be 1.

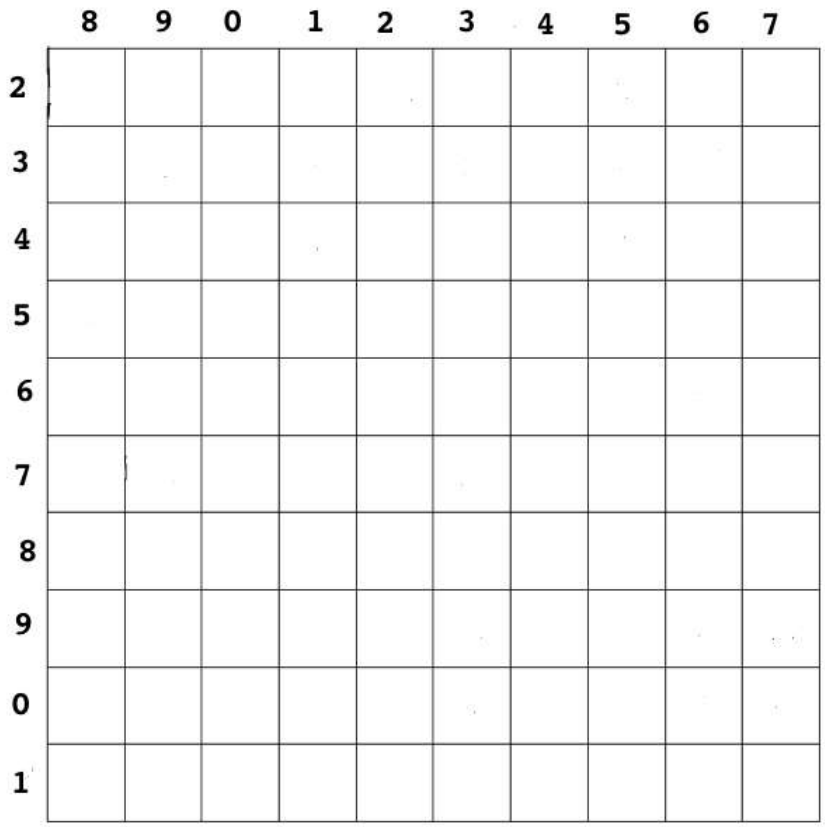
A typical Message Key would look like this: (A302v8>4)

and encoded would look like this: (21 93 40 34 07 84 98 89)

and decoded would read like this:

Pad ID = A30
Row 2=0, and 3=1, 4=2, 5=3, 6=4,7=5, 8=6, 9=7, 0=8, 1=9
Column 8=0, and 9 =1, 0=2, 1=3, 2=4, 3=5, 4=6, 5=7, 6=8, 7=9
Level or Depth = 4 No character = 1

So the Pad would look like this:



This way the same Pad can be used multiple times just by changing the Message Key Setup, without compromising the PAD or the encoded Message. Pad ID Identifies the PAD to use, and the Row/Column Section, sets up the Row/Column Addresses. Level setsthe Depth of PADs used to encrypt the message.