Tactical Communications Procedures

In the past, military units used drum signals and bugle calls to communicate orders on the battlefield. Colonial Militia and Light Infantry units often used whistle commands for the same purpose and such signals can still be used today to coordinate small unit actions like raids and ambushes. Military communications may take the form of visual signals, sound signals, radio messages, telephone conversations or written messages delivered by courier. Since two-way radios are the primary means of modern tactical military communications, this information paper primarily concerns radios, but many procedures apply equally to field telephones used in semi-permanent or defensive positions.

Basic Overview of Radio Types. U.S. Military forces use small handheld radios (like the AN/PRC-126) or backpack radios (like the AN/PRC-77 or AN/PRC-119) with low power and limited range down to the squad and even fire team level, while higher echelons with a need to communicate with more units over greater distances use more sophisticated and powerful radios. Older tactical military radios operated in the VHF FM frequency range of 30.00 to 75.95 megahertz (MHz), while newer radios extend the range up to 87.975 MHz giving 2320 channels. While not approved by higher headquarters, it is not uncommon for U.S. military troops to use privately purchased hands-free voice-activated (VOX) radios, like the Maxon 49 MHz Tracker radios (about $40 to $70) with a 1/4-mile range, for coordination of operations at the platoon level and lower. Such short range VOX transceivers are in wide use by police SWAT teams and would also be useful for Militia tactical operations. Handheld or mobile Citizens Band radios (about $40 to $150) operating in the 26.965 to 27.405 MHz frequency range can also be used for short range tactical communications, but their use should probably be restricted to training and administrative control functions, like vehicle convoys or firing range operations. Under certain conditions, background noise on the AM Citizens Band can make it virtually impossible to communicate even a half-mile away. A better choice for Militia use than a standard CB would be a Single-Sideband (SSB) transceiver (about $170), which gives all the functions of a CB and can also transmit in Upper Sideband (USB) and Lower Sideband (LSB) modes. A standard CB radio transmits a signal when the mike is keyed, which wastes power and reduces its range. In SSB transmission modes, almost no signal is sent until the operator starts talking, giving an effective power of about three times an ordinary CB. With a 102" stainless steel whip antenna an SSB radio has a range of about 30 to 35 miles under all but the noisiest conditions. Single-Sideband radios can usually be fine-tuned in 1-kilocycle increments between each channel, which effectively gives a capability of 400 channels instead of 40 and three transmission modes (CB, USB and LSB). Outlaw CB operators frequently make use of a wider frequency range than allowed by the FCC by transmitting above or below the allowed CB frequencies using illegally modified or imported radios. They also illegally increase output power by using linear amplifiers of 1000 watts or more (although 100 to 300 watts is the norm). Without a proper antenna a linear amplifier can destroy a CB radio. Since out-of-band and excessive power violations of the FCC rules can result in substantial fines and even imprisonment, such illegal setups are not recommended and can only be justified by a genuine survival emergency. If you need more range and power than CB, get an FCC Amateur Radio license, which will open a wide array of other communications options. If you don't want to learn Morse code, you can take

two written exams on FCC rules, basic electronics and radio theory (study materials are available at Radio Shack) and get a no-code Technician license. With a 5-word-per-minute Morse code exam you can upgrade to Technician-Plus class and will be allowed to transmit continuous wave (CW) Morse code, which can get messages through conditions that prevent voice communications. Either Technician class license will allow you to use probably the best type of radio for Militia tactical communications; the VHF FM 2-meter band (144 to 148 MHz frequency range). There is a wide network of repeaters in the 2-meter band that will allow you to extend the range of your radio communications by rebroadcasting your signal on a different frequency at a higher power, usually from a high terrain location. Some repeaters will also allow autopatch connections to the commercial telephone system. Many 2-meter band radios feature the continuous tone-coded squelch system (CTCSS) which lets you program your radio to ignore all calls that don't send a particular sub-audible tone you select. Many 2-meter band radios can also use dual-tone multi-frequency (DTMF) tones to selectively make calls to a particular station or different groups of stations. Radio communications on the same frequency where only one station can transmit at a time (like CB) are called simplex. Communications where both stations can transmit at the same time (like a telephone) are called duplex. Most 2-meter band radios are capable of duplex operation by transmitting and receiving on different frequencies and some can be programmed to automatically jump periodically between different frequencies, which makes unwanted monitoring more difficult. The 2-meter band can make use of packet signals using digitized voice or digital communications between computers. Such digital communications can provide the highest degree of privacy and security for your messages; more about this in the section on codes. Handheld 2-meter radios can often be fitted with either a separate microphone or VOX headset for belt or backpack mounting and can be used with an amplifier and better antenna, giving increased range for base or vehicle use. Radio Shack sells a 2-meter band handheld for $260 (plus $120 for a 30-watt amplifier and $40 for a vehicle type antenna) and a 45-watt mobile transceiver for $350. A test of an ICOM 25-watt 2-meter band radio by "American Survival Guide" using a simple mobile antenna from a 19th floor apartment reported reliable communications in the 40 to 50 mile range, but stated that results will vary with terrain and antenna quality. 2-meter band radios can usually receive a wide range of VHF signals (allowing you to monitor police and other emergency broadcasts) and may be capable of transmitting above or below the authorized band in an emergency endangering life or property. Regular use of the military VHF frequencies outside the 2-meter band requires licensing by the appropriate military agency concerned with the Military Affiliate Radio System or the Civil Air Patrol. Whether you choose CB, Single-Sideband or 2-meter VHF FM for your Militia tactical communications, for field use it would be useful to have a mobile vehicle type transceiver rigged to a backpack mount with a rechargeable battery pack and with both a short range walkie-talkie type antenna and a longer range whip antenna.

Radio Equipment Use. Factors that affect the range of radios are weather, terrain, power, antenna, and the location of the radio. Manmade objects such as buildings and bridges may adversely affect radio transmission. Interference may also come from power lines, electrical generators, bad weather, other radio stations, or enemy jamming. You can correct many of the causes of poor radio communications by using common sense. For example, make sure you are not trying to communicate from under a steel bridge. However, some precautions you must take when using radios are not intuitive. For efficient operation and to prevent equipment damage you should avoid contact with an antenna while transmitting, you should never transmit without an antenna being connected, radio sets should be turned off prior to

starting a vehicle, whip antennas must be maintained in a vertical position during use and must be stowed so they don't contact power lines during transport. Equipment maintenance precautions include insuring plugs and jacks are clean, antenna and power connections are tight and batteries are fresh.

Rules for Radio Use.

* Listen before transmitting and release the push-to-talk button immediately after speaking.
* Make messages clear and concise. Know what you are going to say and, if possible, write messages out before transmitting.
* Speak clearly, slowly, and in natural phrases, distinctly enunciating each word. If the receiving operator must transcribe, allow time for writing.
* Always assume the enemy is listening.

Procedure Words. Standard procedure words (prowords) are used in military communications to keep transmissions as short and clear as possible. For instance, you say WILCO instead of YOU GOT IT DUDE and you never say ROGER WILCO OVER AND OUT when you should say WILCO OUT. Some prowords have different meanings depending upon which band of the radio spectrum you are using. BREAK on the Citizens Band means you want to transmit on a particular channel (e.g. BREAK 35), while on the licensed amateur radio bands it means an emergency transmission which takes priority over routine traffic (e.g. BREAK - EMERGENCY - BREAK). The proword BREAK on military networks means separation of the message text from other parts of a message. The definitions of prowords commonly used in military communications are printed at the end of this paper.

Pronunciation of Letters and Numerals. To prevent misunderstanding by the receiving station, spell difficult words using the phonetic alphabet (printed at the back of this paper). For example: PIDCOKE, I SPELL - PAPA INDIA DELTA CHARLIE OSCAR KILO ECHO - PIDCOKE. In military communications, the phonetic alphabet is also used to transmit five-letter code groups in encrypted messages. Numbers in radio messages, such as times, grid coordinates and call signs, are spoken digit by digit and are pronounced as shown at the back of this paper.

Communications Security. Radio communications are always subject to intercept by enemy forces, so security rules and discipline are strictly enforced on each military radio network by a Net Control Station (NCS; usually the highest headquarters on the net). Since operational requirements may limit the security measures that can be used, rules governing communications security do not guarantee security in every conceivable situation. However, a satisfactory degree of security can be obtained by sensible application of security rules. Whenever possible electronic scrambler or encryption units are used. Even if the rest of a transmission is made in clear language, critical numbers like times, unit status and grid coordinates are manually encrypted and sent using an authorized code. In addition to encryption, prevention of enemy intercept, traffic analysis and direction location is achieved by brevity of transmissions, avoiding excessive radio checks, operating radios on low power with directional antennas, placing intervening terrain between the transmitter and enemy positions whenever possible, and restricting transmissions to certain prearranged times except for dire emergencies. When unknown stations attempt to enter a radio

net, they are challenged with an authentication procedure. Call signs are used in place of plain language unit names. Call signs and frequencies are periodically changed to alternates at prearranged intervals or when directed by the NCS. During the war in Vietnam, many U.S. military units adopted a procedure of using the same one or two word call sign for every station on a radio net and ending each call sign with a number or letter indicating the unit (e.g. 3 for the Third Platoon or D for Delta Company). The suffix 6 usually indicated the Commander's radio operator and 6-ACTUAL meant the Commander himself was speaking. Such lazy procedures gave away too much information to the enemy. A better call sign system identifies each station with a letter, two numbers and a letter, all chosen at random so that enemy analysis of radio traffic will reveal less information. The FCC does not require call signs on the Citizens Band, but it encourages the use of an operator or organization name or the prefix K followed by the operator's initials and residence zip code. Licensed amateur radio operators are encouraged to frequently use their FCC assigned call sign to identify their transmissions and are required to properly identify themselves at least every ten minutes.

Coded Messages. Military radio communications are often conducted using encryption equipment to automatically scramble every transmission. Critical parts of messages sent over tactical radios without encryption equipment are manually encrypted using code tables to deny information to the enemy. The FCC prohibits the use of codes and ciphers to hide the meaning of a message over both the CB and ham radio airwaves; only plain language transmissions are allowed. However, digital packet radio on the ham 2-meter band allows high speed file transfer between computers. A computer file could consist of a digitized voice message or a written message which has been encrypted by a virtually unbreakable computer program. A field transmission between two laptop computers using mobile 2-meter ham radios would be the equivalent of a highly secure military radio encrypted burst transmission. It would be difficult for the FCC to prove such a clandestine communication was not simply an ordinary computer program or data file.

Training Sample Code System. Operational codes and authentication tables for use during a crisis resulting in calling out the Militia will be developed by your Militia unit's S-2 Intelligence and Security section and will be distributed by the Communications Officer on a need to know basis only. For training purposes only, two copies of a sample code matrix table and a sample authentication table have been included at the end of this paper. One copy has been filled in as an example and the blank copy is suitable for training use; make extra photo-copies of the blank sample page or have it laminated for use with a grease pencil or water soluble marking pen. The top of the page has a sample code matrix table system with the alphabet and words commonly used in military messages; the bottom of the page has a sample authentication table. As with any Militia training, take care to obey all applicable laws. Remember that transmitting codes over the airwaves is a violation of FCC rules and can result in substantial criminal penalties. There are better uses for your money than paying federal fines and it is hard to fulfill your Militia duty from behind bars. Training practice sending coded messages with low power toy walkie talkies with a 25 to 50 foot range would be a virtually undetectable technical violation or you could use Dixie cup and kite string field phones which haven't yet come under FCC jurisdiction.

Using the Sample Cryptographic Key. Actual military codes and authentication tables are changed daily or whenever there is reason to believe they have been compromised. The sample code and authentication

table system is designed to be easily changed based upon a twelve character cryptographic key. The example page has been filled out using the cryptographic key BLACKHORSE7K. The first ten letters of the key, BLACKHORSE, have been written in the blocks across the top of the authentication table. Any word or phrase with ten letters that do not repeat can be used, such as PATHFINDER or DONKEY FISH. You can use words with repeating letters by simply discarding the letters which repeat or exceed ten letters. For instance the phrase CLINTON SUCKS gives a ten-letter keyword of CLINTOSUCK. The number 7 found in the 11th position of the cryptographic key has been written at the top of the left column of the authentication table and the blocks below have been filled-in with the next higher number; when the number nine was reached, the next block was filled-in with zero. The letter K found in the 12th position of the cryptographic key has been written in the lower left block of the code matrix table; the rest of the alphabet was then written in the blocks above and across the top of the code matrix, starting over at A when Z was reached.

Using the Sample Code Matrix Table. To use the sample code system to encrypt a message, find the letter or word you need in one of the blocks and look to the left to find the letter for the row; then look for the letter at the top of the column. For example, the letter Q is encrypted as UZ and the word PLATOON is encrypted as SA. When two or more letters or words are found on the same row, do not repeat the left column letter. For example, the phrase BLACK HELICOPTER is encrypted as VXHWYGMB. When transmitting an encrypted message, send it as five letter code groups (filling in the last group with extra punctuation if necessary) preceded by the proword GROUPS and the number of code groups. For example, you say GROUPS ONE ONE PIMXU JMAQD VYDUD AVYDR YUFVW YUXCG RXTXF VWUYA TFZRW TDAPH RFTHG. Spell out the code groups with the phonetic alphabet (e.g. the first code group above is spoken as PAPA INDIA MIKE X-RAY UNIFORM) The above message translates as ENEMY TANK & APC ATTACK CHURCH LOCATION WACO TX DATE 19 APR 93 REPORT 74 CIVILIAN KIA. The sample code matrix would be harder for an enemy to break if the alphabet were spread over more rows and if the row and column letters were not sequential (naturally, this would require a much longer cryptographic key).

Using the Sample Authentication Table. The authentication table at the bottom of the sample page is used to challenge other stations to prove their identity. The authentication procedure is used by a Net Control Station when other stations request permission to enter its radio net. When an unknown or suspected station attempts to communicate with any station, it may be challenged by saying AUTHENTICATE and giving them a two character authentication code. Using the authentication table, pick a random column and row combination and find the letter in the block where they intersect. If the challenge is AUTHENTICATE HOTEL TWO, then the suspected station would properly respond I AUTHENTICATE LIMA. The row of numbers below the keyword on the sample authentication table is designed to be used to provide a degree of security for numbers in tactical messages that are otherwise transmitted unencrypted in plain language. For example, instead of saying RENDEZVOUS AT GRID DELTA FOXTROT 385644, you would say RENDEZVOUS AT GRID DELTA FOXTROT CHARLIE SIERRA HOTEL OSCAR KILO KILO. The ten letter keyword can be given to patrols or individuals to use even if they don't have the entire code matrix and authentication table.

Military Radio Message Formats. Many tactical radio communications take the form of informal

conversations relaying information and orders, although Net Control Stations still have the responsibility for enforcing security procedures and the use of proper prowords and call signs. Some messages follow a set protocol, like calling for and adjusting artillery or airstrikes and the reporting of nuclear, biological and chemical information. Reports on the sighting of enemy forces are often made using the word SALUTE as a memory aid; Size, Activity, Location, Uniform, Time and Equipment. Formal military messages are usually passed over strategic communications systems, but may also be sent over tactical radio nets. Such messages are transmitted in the following format:

(distant station call sign) THIS IS (your call sign)
(message precedence; ROUTINE, PRIORITY, IMMEDIATE or FLASH)
(date-time group; ddttttz month yy. Numbers are individually spoken and the time is given using 24-hour military time. The letter z above represents the time-zone indicator; ZULU for Greenwich Mean Time or LIMA for local time at the sending station.)
FROM (your call sign or the message originator's call sign if you are relaying traffic)
TO (message addressee call sign; not necessarily the call sign of the distant station you are talking to, since they may have the responsibility for relaying traffic to the addressee)
BREAK (this proword separates the text from the rest of the message)
(message classification; UNCLASSIFIED, CONFIDENTIAL, SECRET or TOP SECRET)
(message text)
BREAK
OVER

To send a priority message (which would take precedence over routine traffic on the net) you contact the distant station and state the precedence of the message you wish to send. For example, if you have a message for S20A, your call sign is Z94D and you are calling D81D (either the NCS or another station in your net responsible for relaying traffic to S20A) you would say:

DELTA AIT WUN DELTA - THIS IS ZULU NINER FOWER DELTA - PRIORITY OVER.

The distant station would respond:

ZULU NINER FOWER DELTA - THIS IS DELTA AIT WUN DELTA - OVER.

You would then send your message like this sample:

DELTA AIT WUN DELTA - THIS IS ZULU NINER FOWER DELTA.
PRIORITY
TIME ZERO SEVEN TOO WUN TREE FIFE ZULU JULY NINER SIX.
FROM ZULU NINER FOWER DELTA.
TO SIERRA TOO ZERO ALPHA.
BREAK
UNCLASSIFIED.

ENEMY AMBUSH LOCATION RUBY RIDGE IDAHO DATE TOO WUN AUGUST NINER TOO REPORT WUN ENEMY KILO INDIA ALPHA WUN FRIENDLY CIVILIAN KILO INDIA ALPHA. ENEMY SNIPER ATTACK SAME LOCATION DATE TOO TOO AUGUST NINER TOO REPORT ONE FRIENDLY CIVILIAN KILO INDIA ALPHA TOO FRIENDLY CIVILIANS WHISKEY INDIA ALPHA.
BREAK
OVER

The distant station would then give you a receipt for your message by saying:

ZULU NINER FOWER DELTA - THIS IS DELTA AIT WUN DELTA. ROGER. OUT.

It is important that every military unit be able to shoot, move and communicate. Learning more about two-way radios and tactical communications procedures will allow you to better serve your community as a well trained and prepared Militia member.

Commonly Used Military Prowords:
ALL AFTER - Part of the message to which I refer is all of that which follows ...
ALL BEFORE - Part of the message to which I refer is all of that which precedes ...
AUTHENTICATE - Station called is to reply to the challenge that follows.
AUTHENTICATION IS - Transmission authentication of this message is.
BREAK - I now separate the text from other parts of the message.
CORRECT - What you have transmitted is correct.
CORRECTION - There is an error in this transmission. Transmission will continue with the last word correctly transmitted.
DISREGARD THIS TRANSMISSION - This transmission is in error; disregard it.
DO NOT ANSWER - Stations called are not to answer with a receipt for this message, or otherwise to transmit in connection with this message. When this proword is used the transmission will end with OUT.
GROUPS - This message contains the number of five-letter code groups indicated by the numeral following.
I READ BACK - The following is my response to your instructions to read back.
I SAY AGAIN - I am repeating transmission or part indicated.
I SPELL - I shall spell the next word phonetically.
I VERIFY - The following message (or portion) has been verified at your request and is repeated. Used only as a reply to VERIFY.
MESSAGE - A message that requires recording is about to be transmitted. Not used on nets primarily used for conveying messages; intended for use on tactical nets.
MORE TO FOLLOW - Transmitting station has additional traffic for the receiving station.
OUT - This is the end of my transmission to you and no answer is required or expected.
OVER - This is the end of my transmission to you and a response is necessary. Go ahead: transmit.
RADIO CHECK - What is my signal strength and readability?
READ BACK - Repeat this transmission to me exactly as received

. RELAY TO - Transmit this message to all addresses or to the address designations immediately following.
ROGER - Have received your last message satisfactorily, loud and clear.
SAY AGAIN - Repeat all of your last transmission. Followed by identification data means "REPEAT (portion indicated)".
SILENCE - Cease transmission on this net immediately. If repeated three or more times, silence will be maintained until lifted.
SILENCE LIFTED - Resume normal transmissions. Silence can only be lifted by the station imposing it or by higher authority. When an authentication system is in force, the transmission imposing and lifting silence is to be authenticated.
SPEAK SLOWER - You are transmitting too fast: slow down.
THIS IS - This transmission is from the station whose designator immediately follows.
TIME - That which immediately follows is the time or date-time group of the message.
UNKNOWN STATION - The identity of the station with whom I am trying to establish communications is unknown.
VERIFY - Verify entire message (or portion indicated) with the originator and retransmit correct version. Used only at the discretion of the addressee of the questioned message.
WAIT - I must pause for a few seconds.
WAIT, OUT - I must pause longer than a few seconds.
WILCO - Have received your last message, understand it, and will comply; to be used only by the addressee of a message. Since the meaning of ROGER is included in that of WILCO, the two prowords are never used together.
WORD AFTER - I refer to the word of the message that follows ...
WORD BEFORE - I refer to the word of the message that precedes ...
WORDS TWICE - Communication is difficult; transmit each phrase or code group twice. Used as an order, request or as information.
WRONG - Your transmission was incorrect. The correct version is ...

Phonetic Alphabet:

A Alpha (al'-fah)
N November (no-vem'-ber)
B Bravo (brah'-voh)
O Oscar (oss'-cah)
C Charlie (char'-lee)
P Papa (pah-pah')
D Delta (dell'-tah)
Q Quebec (keh-beck')
E Echo (eck'-oh)
R Romeo (row'-me-oh)
F Foxtrot (foks'-trot)
S Sierra (see-air'-ah)
G Golf (golf)

T Tango (tang'-go)
H Hotel (hoh-tell')
U Uniform (you'-nee-form)
I India (in'-dee-ah)
V Victor (vic'-tah)
J Juliett (jew'-lee-ett)
W Whiskey (wiss'-key)
K Kilo (key'-loh)
X X-Ray (ecks'-ray)
L Lima (lee'-mah)
Y Yankee (yang'-key)
M Mike (mike)
Z Zulu (zoo'-loo)

Phonetic Numbers:
1 wun
6 six
2 too
7 sev'-en
3 tree
8 ait
4 fow'-er
9 nin'-er
5 fife
0 ze'-ro
44 fow'-er fow'-er
90 nin'-er ze'-ro
136 wun tree six
500 fife ze'-ro ze'-ro
1200 wun too ze'-ro ze'-ro
1478 wun fow'-er sev'-en ait
7000 sev'-en tou'-sand
16000 wun six tou'-sand
812681 ait wun too six ait wun

**[The sample code matrix and authentication systems described in the text of the information paper were printed on two pages; one sample page was filled-in as described in the text and the other was left blank for training use. To reconstruct the code system, at the top of the page make a table with 12 rows and 16 columns. Write the 26 letters of the alphabet, the numerals 0 through 9, some punctuation and words commonly used in military messages in the blocks. You can fill-in the blocks however you choose, but if you don't use the sample below, then the examples in the text will not be correct. Make an extra row above these blocks and an extra column to their left and leave them blank; these will contain your cryptographic key as described in the text. The authentication table at the bottom of the page has ten

rows and ten columns. Fill in the 100 blocks with random letters of the alphabet. Use the example below or correct the text example to match your system. Make an extra row at the top of the table and place the numbers 0 through 9 left to right in these boxes. Make a blank extra row at the top and a blank extra column to the left for the cryptographic key. To the right of the authentication table you should have room for six lines to be filled in by the radio operator. Label these lines Call Sign, Alternate Call Sign, Radio Frequency, Alternate Radio Frequency, Net Control Station Call Sign, and Alternate NCS Call Sign. Make two copies of this page; leave one blank and fill the other in using the cryptographic key BLACKHORSE7K in the manner described in the text.]**

[The blocks in our training sample code matrix were filled-in as follows (separated by the backslash character)]

row 1 A \ B \ C \ D \ E \ F \ G \ H \ I \ J \ K \ L \ M \ ?
row 2 N \ O \ P \ Q \ R \ S \ T \ U \ V \ W \ X \ Y \ Z \ &
row 3 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ + \ # \ odd \ even
row 4 UNIT \ patrol \ team \ squad \ platoon \ company \ battalion \ leader \ commander \ detachment \ attached \ forward observer \ medic \ med-evac
row 5 REPORT \ date time \ coordinate location \ personnel \ weapons \ ammo \ food \ water \ equipment \ KIA dead \ WIA wounded \ MIA missing \ POW captured \ radio frequency
row 6 OPERATIONS \ raid \ recon \ ambush \ move to contact \ assemble \ fortified \ attack \ defend \ patrol base \ link-up \ listening post \ observation post \ meeting
row 7 MISSION \ HQ headquarters \ security \ support \ assault \ junction \ building(s) \ crossing \ road \ trail \ forces \ civilian(s) \ enemy \ friendly
row 8 STATUS \ execute start \ terminate finish \ halt stop \ prepare ready \ move go to \ help urgent \ successful \ failed \ aborted \ detected \ waiting \ yes \ no
row 9 DISPOSITION \ change \ new \ we my \ you your \ they their \ send need \ spot observation \ in-position \ lost \ found \ easy \ difficult \ unknown
row 10 TRANSPORT \ tank \ truck \ wheel \ track APC \ helicopter \ plane \ ground \ air \ water \ foot \ vehicle \ paratroop \ heliborne air assault
row 11 MILITARY TERM \ objective \ rallying point \ release point \ target reference point \ line of departure \ phase line \ command post \ area of operation \ by-pass \ enroute \ dig-in \ contact \ break rest
row 12 MILITARY TERM \ signal \ depart \ return \ occupy occupied \ escape & evade \ watch out \ check check-out \ silent \ delay \ cancel \ immediate \ conduct \ withdraw retreat

[The blocks in our training sample authentication system table were filled-in as follows (separated by the backslash character)]

row 1 J \ B \ O \ Y \ I \ K \ M \ D \ S \ J
row 2 U \ R \ C \ L \ A \ O \ B \ Y \ Q \ D
row 3 W \ C \ X \ E \ G \ H \ W \ N \ D \ Z
row 4 B \ N \ F \ R \ T \ S \ C \ I \ R \ P
row 5 U \ J \ V \ F \ I \ X \ T \ C \ M \ O
row 6 R \ P \ B \ M \ S \ L \ M \ N \ S \ A

row 7 T \ P \ E \ Q \ A \ I \ O \ E \ P \ X
row 8 F \ J \ Q \ N \ V \ Z \ U \ W \ L \ Q
row 9 Y \ H \ D \ V \ G \ G \ L \ U \ K \ E
row 10 G \ K \ H \ F \ A \ K \ V \ Z \ T \ H