

GBPPR 'Zine



Issue #109 / The Monthly Journal of the American Hacker / May 2013

"It is difficult to go a few days without being accosted by a member of a radical left-wing organization like the Eastern Service Workers Association or the Revolutionary Communist Party. The most active political group on campus, or at least the most prolific distributor of material, is the International Socialist Organization. Even professors adorn their offices with slogans such as 'Marx was Right', or 'We Are the 99%'."

— December 1, 2012 quote from "UMass Boston's Left Wing Radicalism Mirrors Communism."

(umassmedia.com/opinions/article_2e95b0c0-3c05-11e2-9ee4-001a4bcf6878.html)

Table of Contents

- ◆ **Page 2 / Centrex Data Facility Pooling – Implementation Procedures / #1A ESS – Part 2**
 - ◆ Procedures for implementing Centrex data facilities under a #1A ESS.
- ◆ **Page 30 / Techniques for Countering Thermal Imaging Devices**
 - ◆ Collection of experimental ideas and techniques to counter thermal imaging devices.
- ◆ **Page 38 / Battlefield Laser Warning Receiver**
 - ◆ Experimental device to detect the laser designator used by laser-guided bombs and missiles.
- ◆ **Page 55 / Bonus**
 - ◆ Bias Bingo
- ◆ **Page 56 / The End**
 - ◆ Editorial and rants.

AT&T 231-318-360

7. CDFP FEATURE IMPLEMENTATION

The CDFP feature implementation (Fig. 15) involves six major areas: trunk translations, routing translations, centrex translations, line-related translations, miscellaneous translations, and traffic/plant measurement translations.

7.1 Establish New Outgoing Trunk Group for SD-6A013-01 or SD-6A019-01

7.1.1 Verify Trunk Group

See Fig. 16. Verify that TG (trunk group) is not established by typing

VFY-TKGN-14 aaa.

aaa = TG number (Form ESS 1229A2, columns 35-37).

Observe the TR10 output message (Fig. 17) indicating that TG is not established.

7.1.2 Verify TNN Correctly Equipped

Verify that each TNN is correctly equipped by using the VFTNNSVY input message. Refer to 6.1 for details.

Verify 1-port miscellaneous equipment as follows.

- (1) Compare Form ESS 1229/1230 with TR14 output message data. If TR14 data is incorrect, TNN(s) is not correctly equipped.
- (2) If a TR12 output message (Fig. 18) did not also print, go to Step (3). If the TR12 message was also printed out, determine whether the TR12 data is correct. If not, TNN(s) is not correctly equipped.
- (3) For each supervisory scan point found in the TR14 output message, type

VFY-MSN-13 aa bb cc.

aa = Master scanner frame (00 through 63)
bb = Master scanner row (00 through 63)
cc = Master scanner column (00 through 15).

- (4) Determine whether TR12 output message data (Fig. 18) is correct. If not, TNN(s) is not correctly equipped.

ISS 1, AT&T 231-318-360

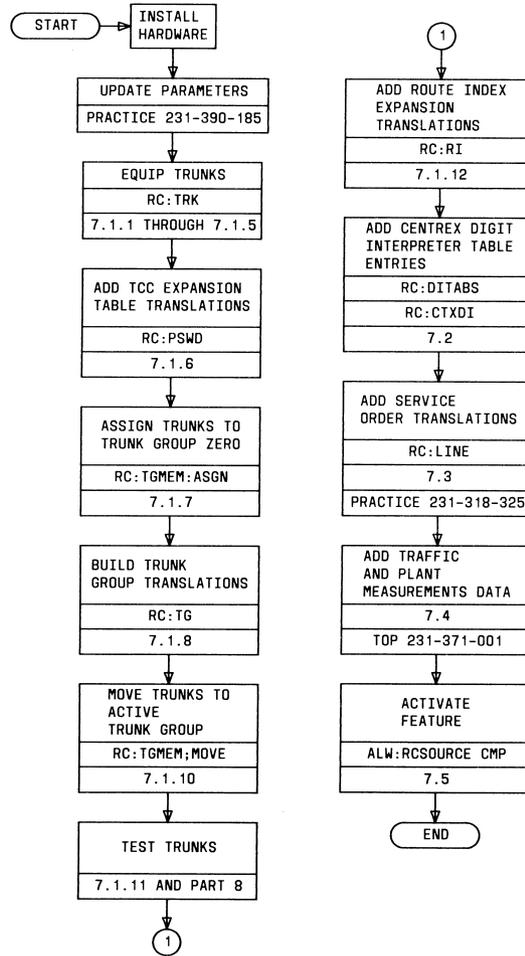


Fig. 15 — CDFP Feature Implementation

AT&T 231-318-360

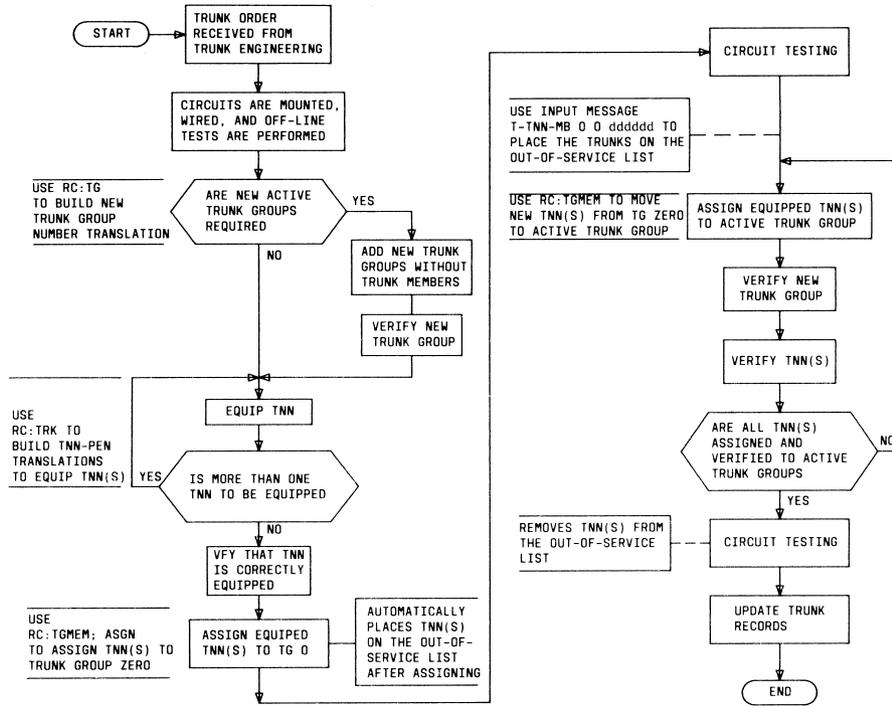


Fig. 16 — General Flowchart to Add a Trunk Circuit

ISS 1, AT&T 231-318-360

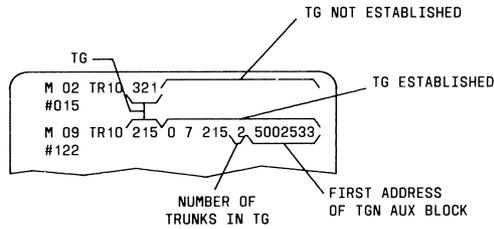


Fig. 17 — Example of TR10 Messages

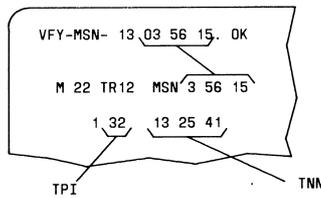


Fig. 18 — Example of TR12 Message

7.1.3 Verify TNN Assignment

Verify that each TNN is unassigned or assigned to TG 0. Proceed as follows.

- (1) From TR14 output message (Fig. 11), determine if TNN assignment is correct. If not, refer problem to network administration personnel.
- (2) Proceed only if TNN assignment is correct.

7.1.4 Busy TNNs

Make each TNN maintenance busy. If all trunks in the entire TG are to be made busy, perform Steps (1) and (3); if not, perform Steps (2) and (3) at MTCE terminal.

- (1) To busy all trunks in the entire TG, type

TRK-GROUP-MB 00 aaaa.

AT&T 231-318-360

aaaa = Trunk group.

Note: Trunks in TG zero should not be made busy with the TRK-GROUP-MB message.

- (2) For each trunk to be made busy, type

T-TNN-MB 00 nnnnnn.

nnnnnn = TNN.

- (3) If TRK-GROUP-MB message was input, observe TN15 and TN05 output messages for each TNN not put on the out-of-service list. If T-TNN-MB message was input, observe TN06 output message for each TNN made busy.

7.1.5 Equip TNNs

Properly equip each unequipped TNN as follows.

- (1) Construct RC message per Table A and Fig. 19.
- (2) At terminal, type RC message as constructed in Step (1) and observe RC18 5 0 ACPT response.

If necessary, properly equip each TNN that is incorrectly equipped. Proceed as follows.

- (1) If TNN is to be changed, verify new TNN is unassigned by typing the following message and observe TR14 output message (Fig. 11).

VFY-TNN-11 bbbbbb.

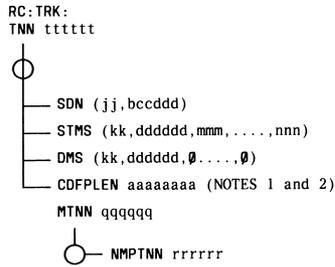
bbbbbb = New TNN.

- (2) Construct RC message per Table A and Fig. 20.

Note: The mate TNN can only be removed by an RC:TRK;OUT: message. Refer to Step (5).

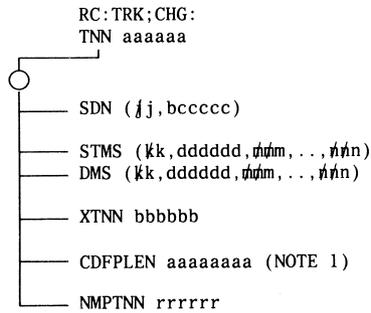
TABLE A				
RC:TRK:-1-PORT TRUNK KEYWORDS				
RC MESSAGE	FORM ESS	COLUMN	REMARKS	
RC:TRK:	—	—	Message heading	
TNN ttttt	1230	16-21	ttttt = trunk network number (TNN)	
	1229A2	29-34		
SDN (jj,Mccddd)	1229A1	28-29	jj = quantity of SD points: = 2 for PFP = 3 for NMP	Signal distributor (SD)
		25	M = SD type	
		26-27 and 30-32	ccddd = first SD point	
STMS (2,dddddd,m,n)	1229A1	35-36	2 = quantity of master scanner points	Supervisory scan point data
		33-34 and 37-40	dddddd = scan point number	
		—	m, n = TPIs for master scanner points 0 and 1 respectively: = 31,32 for CPI 223 = 31,43 for CPI 227	
DMS (1,dddddd,0)	1229A1	43-44	1 = quantity of master scanner points	Directed scan point data
		41-42 and 45-48	dddddd = scan point number	
			0 = TPI value for directed scan point	
CDFPLEN aaaaaaaa	1230	33-40	aaaaaaaa = CDFP auxiliary LEN	
MTNN qqqqqq	1230	41-46	qqqqqq = mate TNN of TNN keyword	
NMPTNN rrrrrr	1230		rrrrrr = NMP TNN (1AE9 and later only)	
XTNN bbbbbb	1229A2	29-34	bbbbbb = TNN to replace TNN ttttt (on change message only)	
	1230	16-21		

AT&T 231-318-360



- NOTES:
1. The CDFPLEN must be assigned and have an originating major class of 42.
 2. The CDFPLEN will be assigned in the LEN translator if input in this message.

Fig. 19 — Equipping a 1-Port Miscellaneous Trunk



- NOTE:
1. If CDFPLEN is input in this message, the old CDFPLEN will be unassigned and the new CDFPLEN will be assigned in the LEN translations.

Fig. 20 — Changing a 1-Port Miscellaneous Trunk

- (3) At terminal, type RC message as constructed in Step (2) and observe RC18 5 0 ACPT output response.
- (4) Verify that each TNN is now correctly equipped by using the VFTNNSVY input message. Refer to 6.1 for details.
- (5) If necessary, use the following RC message to unequip trunk(s).

```
RC:TRK;OUT:  
TNN aaaaaa!  
  
aaaaaa = TNN.
```

Note: As result of this message, the trunk(s) is unequipped and the CDFPLEN is unassigned.

7.1.6 Add TCC Data

If TCC (Form ESS 1204) is to be added for TG, perform the following steps.

- (1) If new TCC is to be added, check length of TCC expansion table as follows:
 - (a) At terminal, type

```
DUMP:CSS,ADR 7720411;DEC!
```
 - (b) From DUMP:CSS output message, determine length of TCC expansion table.
 - (c) From Form ESS 1204A, determine highest number TCC.
 - (d) Multiply highest TCC by 4.
 - (e) Add 4 to the results of Substep (d) to determine required length of table to add new TCC data.
 - (f) Determine whether required table length is less than active table length [Substep (b)]. If so, active table length is sufficient. If not, active table length is insufficient to add new TCC data.
 - (g) If active table length is insufficient to add new TCC data, move TCC expansion table to increase table length. Refer to AT&T Practice 231-367-020 for procedure, then return to Step (2).
- (2) Add TCC to TCC expansion table as follows:
 - (a) Obtain TCC from Form ESS 1204 (see sample, Fig. 4).
 - (b) Multiply TCC by 4 (results = iiii). Retain results iiii for use in Substep (e).
 - (c) From Form ESS 1204 (Fig. 4), identify translation words for which data is to be changed (Translation word 1, 2, 3, or 4).
 - (d) Determine new data by converting binary word in INPUT row to octal for each translation word being changed (results = ddddddd). (See Fig. 4.) Save results for use in Substeps (h) and (i).
 - (e) Determine address and old data of translation words being added or changed by typing the following message:

AT&T 231-318-360

DUMP:CSS,INDIR 1,ADR 7720011,INC iiiii,L4!

iiii = Results obtained in Substep (b).

Note: If new TCC is being added, old data of translation words may be all zeros.

- (f) From DUMP:CSS output message, determine address of TCC translation words (Fig. 21) (results = bbbbbb). Retain results for use in Substeps (h) and (i).
- (g) From DUMP:CSS output message, also determine old data (contents) contained in TCC translation words (Fig. 21) (results = cccccc). Save results for use in Substeps (h) and (i).
- (h) Construct RC message per Table B and Fig. 22. Check for accuracy.

Caution: Extreme caution must be exercised in using RC:PSWD message to avoid errors resulting in bad translations data.

- (i) At terminal, type RC message as constructed in Substep (h) and observe RC18 1 0 ACPT response.

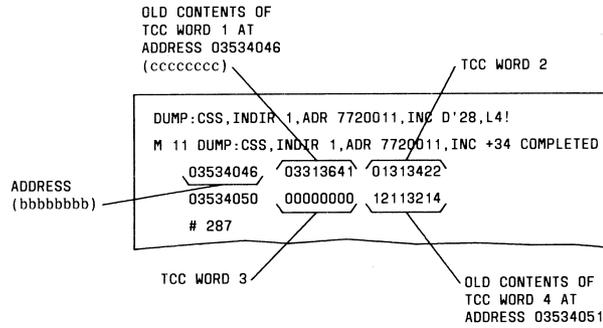


Fig. 21 — Example of DUMP of TCC Translation Words

TABLE B	
RC:PSWD KEYWORDS	
RC MESSAGE	REMARKS
RC:PSWD:	Message heading
ADD bbbbbb	bbbbbb = address of memory to be changed.
OLDDAT cccccc	ccccc = old data determined from DUMP:CSS output message
DAT ddddddd %	ddddddd = octal form of binary number found in form and converted to octal
% Repeatable segment. If more than one word is to be changed and addresses for each word are consecutive, all word changes can be entered in same message by repeating; otherwise, must be entered one word at a time.	

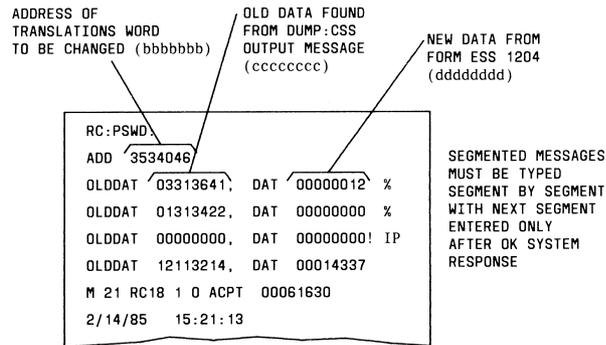


Fig. 22 — Example of RC:PSWD Message for Multiple Changes

(3) Verify TCC expansion table data as follows.

(a) At terminal, type

```
VF:DATA:
FROM 7720011
NWDS 1
DUMP!
```

(b) From TR100 output message, obtain starting address of TCC expansion table for use in Substep (c).

L.

AT&T 231-318-360

(c) Type

```
VF:DATA:
FROM aaaaaa
NWDS 4
DUMP!
```

aaaaaa = Starting address of TCC expansion table + (TCC x 4 converted to octal).

- (d) Compare the four TCC translation words in the TR100 output message with each word on Form ESS 1204.
- (e) For each TCC translation word in error, correct using procedures in Steps 2(h) and 2(i).

7.1.7 Assign Trunks to TG Zero

If some trunks are not assigned to TG 0, assign as follows.

- (1) Construct RC message per Table C and Fig. 23 to assign TNNs to TG 0.

Note: More than one segment of a segmented message may be typed with DATASPEED[®]40 teletypewriter in FORM ENTER mode and then entered, segment by segment, in regular mode.

- (2) At terminal, type RC message as constructed in Step (1) and observe RC18 9 0 ACPT response.
- (3) Verify that each TNN is assigned to TG 0 with correct TCC by using the VF:TNN SVY input message. Refer to 6.1 for details.

TABLE C			
RC:TGMEM;ASGN KEYWORDS			
RC MESSAGE	FORM ESS	COLUMN	REMARKS
RC:TGMEM;ASGN:	—	—	Message heading
TCC mmm } % }	1229A2	41-43	Trunk class code
MEM(0,ttttt) }	1230	16-21	ttttt = TNN. All TNNs assigned to TG 0 have member number = 0 regardless of Form ESS 1202
% }	1229A2	34-39	
% Repeatable segment. More than one can be entered in same message.			

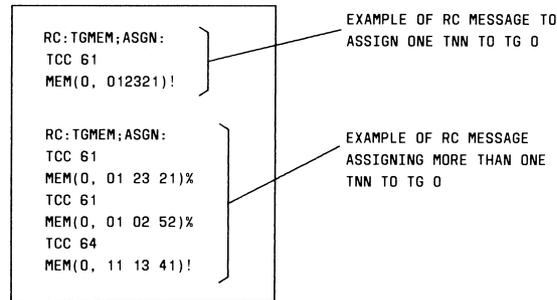


Fig. 23 — Example of Assigning Trunks to TG 0

7.1.8 Build Trunk Group

Establish TG as follows.

- (1) Construct RC message per Table D and Fig. 24 for TG.
- (2) At terminal, type RC message as constructed in Step (1) and observe RC18 2 0 ACPT response.
- (3) Verify TG data in memory by typing

VFY-TKGN-14 aaa.

aaa = TG number.

Observe the TR10 output message (Fig. 17) indicating that TG is established.

- (4) Compare TR10 output message from Step (3) with data obtained from forms in Table D.
- (5) If incorrect data in memory, recheck RC message input data. If incorrect data resulted from RC message input, correct RC message and start over from Step (1).
- (6) Compare verification data in the TR10 output message with the TR14 output message. Insure that the TCCs are the same. If not, check forms for accuracy.
- (7) If TCC(s) are to be changed, unassign TNNs with incorrect TCC(s) per Step (8); then reassign TNN(s) with correct TCC(s) per Table C and Fig. 23 (refer to 7.1.7).
- (8) Unassign TNN(s) per Table E. Then verify TNN(s) using VF:TNNSVY message (refer to 6.1 for details).

AT&T 231-318-360

TABLE D				
RC:TG KEYWORDS				
RC MESSAGE	FORM ESS	COLUMN	REMARKS	
RC:TG:	—	—	Message heading	Columns on ESS forms associated with optional keywords will not contain data if option is omitted. Data in columns 69-80, Form ESS 1216, contain variable information depending on type number in column 65-66.
TG aaa	1229A2	35-37	Trunk group number	
TYP 2	—	—	Trunk group type	
SIZE ddd	1229A2	38-40	ddd = total number of trunks in TG (keyword used only for 2-way or TYP 7 trunks, or if busy verification of trunks or data link group keywords are specified).	
TCC bbb	1229A2	41-43	Trunk class code	
COL gggg	1208	51-54	Chart class column	
ATT hhh	1504	28-30	Automatic trunk test table. For service circuit TG, hhh = 4.	
RAMN aa	1216	69-70	Recorded announcement member number	
RRRI nnnn	1216	69-72	Reroute route index. Type 18 (Form ESS 1216, column 65-66).	
TTY aa	1216	31-32	TG maintenance channel. Channel 13 used as default.	
TTP cc	1216	28-30	Trunk test position (TG test panel member number)	
TXT a	1216	41-42	a = transmission type	
PRECUT	1216	40	Precut bridging during cutover	

ISS 1, AT&T 231-318-360

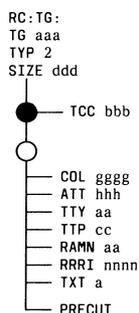


Fig. 24 — RC: TG Message Flowchart

TABLE E			
RC:TGMEM;UNASSIGN KEYWORDS			
RC MESSAGE	FORM ESS	COLUMN	REMARKS
RC:TGMEM;UNASGN:		—	Message heading
MEM(aaa,ttttt)%	1229A2	38-40	aaa = trunk member number*
	1230	16-21	ttttt = TNN
	1229A2	29-34	
% More than one member from same TG can be unassigned in one message * aaa must equal zero if no data in columns 38-40. (No trunk member list exists in TG auxiliary block)			

7.1.9 Verify Trunk Circuit at Frame

At equipment location, verify that trunk circuit with correct schematic drawing number is installed.

Connect trunk distributing frame jumpers for all TNNs.

AT&T 231-318-360

7.1.10 Move Trunk Members to Active TG

Move TNN(s) from TG 0 to active TG as follows.

- (1) Construct RC message per Table F.
- (2) At terminal, type RC message as constructed in Step (1).

Verify each TNN moved to active TG as follows.

- (1) Verify each TNN by using the VF:TNNSVY input message. Refer to 6.1 for details.
- (2) Compare TR14 output message with data on Forms ESS 1230 and 1229. If TR14 data is wrong, correct RC:TGMEM;MOVE message, then retype.
- (3) Verify TG data, type

VFY-TKGN-14 aaa.

aaa = TG number.

- (4) Compare TR10 output message data (Fig. 17) with data obtained from forms.
- (5) If TR10 output message contains an auxiliary block address, proceed as follows:
 - (a) At terminal, type

DUMP:CSS,ADR cccccc,INC -1,L2;BIN!

ccccc = Auxiliary block address.

- (b) From DUMP:CSS output message, determine whether bits 22-18 of the first word of auxiliary block are all zeros. If so, convert bits 9-0 of word before auxiliary block to decimal; subtract 1 from decimal number to determine length of auxiliary block. If bits 22-18 are not all zeros, convert bits 22-18 to decimal to determine length of auxiliary block; if this number is greater than 3, continue on to next step.

TABLE F			
RC:TGMEM;MOVE KEYWORDS			
RC MESSAGE	FORM ESS		REMARKS
	NUMBER	COLUMN	
RC:TGMEM;MOVE:	—	—	Message heading
TOTG rrr	1229A2	35-37	rrr = TG number to which trunk members are being moved
MEM (0,ttttt)%	1229A2	38-40	0 = TG member number
	1230	16-21	ttttt = TNN
	1229A2	29-34	

- (c) At terminal, type

DUMP:CSS,ADR cccccc,L bbbb;BIN!

ccccc = Auxiliary block address
bbbb = Length of auxiliary block.

- (d) From DUMP:CSS output message, convert binary TNNs listed in auxiliary block to decimal.

Note: List of TNNs begins at word 3 (fourth word of DUMP:CSS output).

- (e) Verify that the TNNs listed in auxiliary block agree with those moved to active TG (Form ESS 1229A2).

7.1.11 Test Trunk Members

Verify member list as follows.

- (1) At MTCE terminal, type

TRK-GROUP-LT 00 nnnn.

nnnn = TG number.

- (2) Verify that the TNNs listed in TN15 output message agree with those moved in TG.

Test all trunk members as follows. Perform trunk diagnostic tests per Part 8 and return.

7.1.12 Assign Route Index for CO-IVDM Pool

Assign RI for each CO-IVDM pool as follows.

- (1) Construct RC message per Table G and Fig. 25.
(2) At terminal, type RC message as constructed in Step (1) and observe RC18 3 0 ACPT response.

AT&T 231-318-360

TABLE G		
RC:RI KEYWORDS		
RC MESSAGE	FORM ESS 1303C COLUMNS	REMARKS
RC:RI:	—	Message heading
RI cccc	20-23	cccc = route index
TG bbb	25-27	bbb = trunk group number
NRI aaaa	45-48	aaaa = next route index. = 2047 when columns = STOP
TCC ggg	—	Trunk class code. Used only if trunk group contains no members. Form ESS 1229A2, columns 41-43
FIXED	20-23	Fixed route index. Required when RI is 199 or less
CST ff	39	ff = LO (Low tone, steady)/HI (high tone, steady)/DL (double burst, low tone)/DH (double burst, high tone) class of service
CRC h	40	h = coin return code
FRE	41	Free call when column marked
OPT ii	43-44	ii = options
TATO u	55	u = 0 (column = 1)/1 (column = 3)/ 2 (column = 5)/3 (column = 7) for tone and announce- ment time-out period. Do not use when column = 0
SFMUT	56	Single frequency mutilation flag when column marked

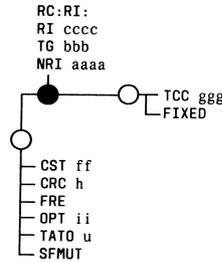


Fig. 25 — RC:RI Message Flowchart

- (3) Idle all trunks by typing the following message for each TNN. At MTCE terminal, type

T-TNN-MI 00 tttttt.

ttttt = TNN.

Observe the TN06 CDFP 0 tttttt dddd ACT response (where tttttt = TNN and dddd = TG number).

- (4) Update office records.

7.2 Establish Centrex DI Table Entries

7.2.1 Determine Required Digit Interpreter Tables

Determine if DI tables exist for required new access codes (data type 5). Proceed as follows.

- (1) Using the new access code (Form ESS 1109A, columns 45-49 for items 0 through 49) as input to the VFY-XDGNT message, verify DI table entries. Refer to 6.2 for details.
- (2) From TR02 output message, determine if the number of digits interpreted (field NDIG) is equal to the number of digits to be interpreted (variable 'c' in 6.2).
 - (a) If so, and all other data equal zeros, then no additional DI tables are required. Go to 7.2.3.
 - (b) If not, go to Step (3).
- (3) If NDIG field is equal to 'n' ('n' being 1, 2, 3, or 4), note that 'n + 1' level DI table is required. If access code (Form ESS 1109A, columns 45-49) contains more digits than 'n + 1', subtract 'n + 1' from the number of digits in access code, this number plus 'n + 1' level DI table is required.

AT&T 231-318-360

Note: If rightmost digit in access code contains a number sign (#), timing table is also required for second highest level DI table.

- (4) Proceed to 7.2.2.

7.2.2 Add DI Tables to Centrex Common Block

Add required DI tables as follows.

- (1) Construct RC message per Table H and Fig. 26.
- (2) At terminal, type RC message as constructed in Step (1) and observe RC18 22 0 ACPT response.

Note: When seizing DI tables, DI levels must be seized in ascending order. All second levels must be seized before third levels, all third levels before fourth, etc. Refer to AT&T Practice 231-318-355 for further information.

TABLE H		
RC:DITABS KEYWORDS		
RC MESSAGE	FORM ESS 1109A COLUMNS	REMARKS
RC:DITABS:	--	Message heading
CTX <i>lllc</i>	25-28	CTX group number
DGS <i>abcdX</i>	45-54	abcdX = DI level to be seized dX = second level cdX = third level bcdX = fourth level abcdX = fifth level
TIME	46-49	Timing table required. Used when last digit in columns equals #. Determined prior to this step.

ISS 1, AT&T 231-318-360

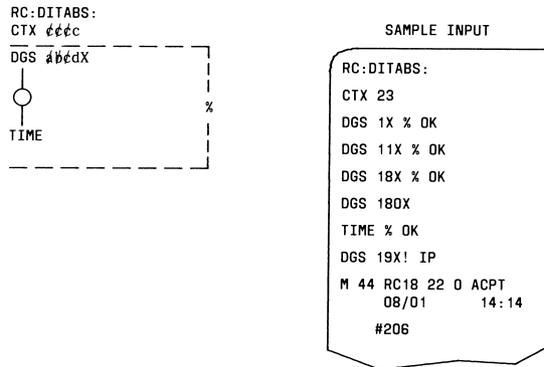


Fig. 26 — RC:DITABS Flowchart and Sample Input

7.2.3 Add Data Type 05 to DI Table

Add data type 05 to DI Table as follows.

- (1) Construct RC message per Table I and Fig. 27.
- (2) At terminal, type RC message as constructed in Step (1) and observe RC18 23 0 ACPT response.

7.2.4 Verify DI Table Entry for Data Type 05

Using the access code (Form ESS 1109A, columns 45-54) as input to the VFY-XDGNT message, verify DI table entries. Refer to 6.2 for details.

If TR02 output message data is incorrect, correct RC message or clear trouble with local TAC or equivalent.

AT&T 231-318-360

TABLE I		
RC:CTXDI KEYWORDS		
RC MESSAGE	FORM ESS 1109A COLUMNS	REMARKS
RC:CTXDI:	—	Message heading
CTX <i>aaaa</i>	25-28	Centrex group number (located in Item 00 of Form ESS 1109A)
DGS <i>dddde</i>	45-49	Access code or start of digit range to be interpreted
DGE <i>ddddf</i>	50-54	End of digit range to be interpreted (if required). Only last digit may differ from digits in DGS.
STYP 30	62-63	Subtype number (for data type 05)
SSTYP <i>aa</i>	69-70	Sub-subtype number: aa = 0 for PFP, 1 for NMP
RI <i>rrr</i>	58-61	Route index for STYP 30
DNYGPS (<i>g,g,g,g,g,g</i>)	36-43	CAT (centrex treatment) codes (0-7) to be denied access to feature. g = CAT code numbers that do not contain check in column for STYP 30.

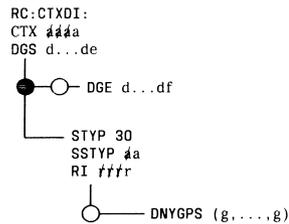


Fig. 27 — RC:CTXDI Message Flowchart

7.3 Add Service Order Translations

Add centrex line (non-MLG) translations for lines per AT&T Practice 231-318-325 and return.

Note 1: The auxiliary LEN must be assigned an originating major class of 42.

Note 2: For the CDFP feature, keywords E2H and EAB must be input in the RC:LINE message to allow flash recognition and call hold, respectively.

Note 3: There can now be TRCs against a DN for CDFP or subscriber line busy peg count prior to RC:CFV messages.

Update office records.

7.4 Assign Traffic and Plant Measurements

Assign traffic and plant measurements and destination codes per AT&T Practice 231-371-001.

Note: There can now be TRCs against a DN for CFV (call forwarding variable) or CDFP prior to RC:TRFSLB (subscriber line busy peg count) messages.

7.5 Activate CDFP Feature

At MTCE terminal, activate the CDFP feature by typing

ALW:RCSOURCE CMP!

CMP = Centrex Modem Pooling; RC source for CDFP.

Observe the REPT:RC SOURCE response.

AT&T 231-318-360

8. TRUNK MAINTENANCE/DIAGNOSTICS

This part covers trunk maintenance/diagnostics for the CDFP OGT circuit(s).

8.1 Testing Objective

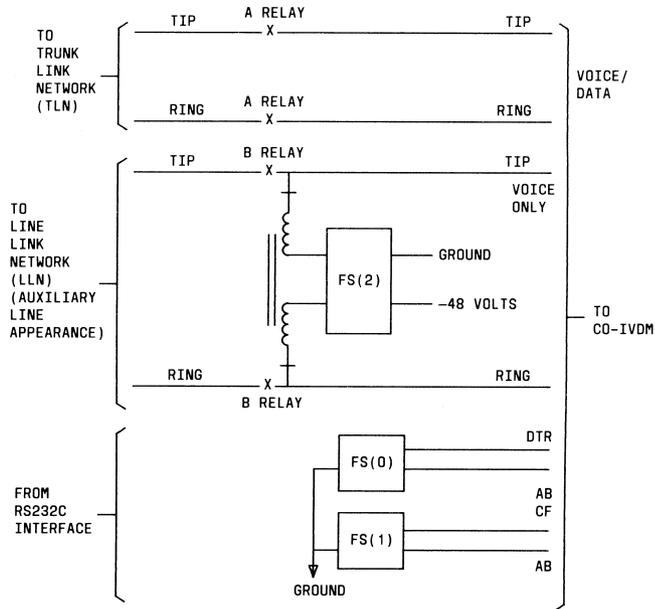
The objective of trunk testing is to aid maintenance personnel in maintaining performance standards of trunk circuits. This is accomplished by detecting trouble conditions and removing faulty trunks from service.

To insure that the CDFP OGT is functioning properly, the major components of the trunk circuits must be monitored. These components consist of 3 scan points and 2 relays which function as follows. (See Fig. 28.)

- FS(0) - Line side supervision: This scan point provides line side supervision toward the CDFP line appearance and monitors data carrier detect RS232C signal. This signal indicates that carrier signal is present from the customer premises IVDM (CP-IVDM) to the host computer. This signal can be detected at the RS232C interface between the CO-IVDM and the CO-CPDS.
- FS(1) - Trunk side supervision: This maintenance/error scan point is used to verify carrier signal sent from the host computer to the CP-IVDM. If not present, the trunk is automatically taken out of service and placed on the H&W (high and wet) list. When carrier is returned, the trunk is automatically restored to service.
- FS(2) - This scan point is used to verify network continuity to the CDFP line appearance. It is also used to detect when a customer goes on hook after a successful data connection to the host computer. After such detection, cut-through is provided to the auxiliary line appearance for subsequent voice calls.
- A relay - The A relay (network continuity) provides for cut-through from the CO-IVDM to the TLN (trunk link network).
- B relay - The B relay (full path continuity) controls two functions: (1) When released, it feeds battery and ground through FS(2) to the CO-IVDM to monitor the CDFP line for on-hook after a data call has been originated. After a successful data connection and the CDFP line goes on hook, the B relay is operated. (2) When operated, it provides cut-through from the auxiliary line appearance to the CO-IVDM. The CDFP line is then supervised for origination at the auxiliary line appearance. And the auxiliary line appearance is checked for busy/idle state on call completion attempts to the CDFP line.

Trunk maintenance/diagnostics consist of the following functions:

- (a) Removing and restoring the CDFP OGT from/to service.
- (b) Running voice and simultaneous voice/data diagnostic tests on suspected faulty trunk circuits.
- (c) Routine testing (voice only) of all trunk circuits via APT (automatic progression testing).
- (d) Limited manual verification of trunk circuits from trunk test positions.



LEGEND:

- A RELAY = FOR NETWORK CONTINUITY
- B RELAY = FOR CUT-THROUGH TO AUX LINE APPEARANCE AND TAKING FS(0) OUT OF LOOP
- FS(0) = FERROD SCAN FOR DTR LEAD OF RS232C INTERFACE
- FS(1) = FERROD SCAN FOR CF LEAD OF RS232C INTERFACE
- FS(2) = FERROD SCAN FOR VOICE SUPERVISION
- DTR = RS232C LEAD THAT SIGNIFIES CARRIER FROM CP-IVDM TO HOST COMPUTER
- CF = RS232C LEAD THAT SIGNIFIES CARRIER FROM HOST COMPUTER TO CP-IVDM
- AB = RS232C LEAD FOR SIGNAL GROUND FOR DTR AND CF LEADS
- CO-IVDM = CENTRAL OFFICE INTEGRATED VOICE/DATA MULTIPLEXER

Fig. 28 — Functional Block Diagram of CDFP OGT

AT&T 231-318-360

8.2 Removing and Restoring OGT Circuits

8.2.1 Removing Trunks from Service

When physically removing a faulty trunk from a frame, both the specified TNN and its mate must be taken out of service before the trunk circuits are pulled from the frame for repair or replacement. This may be accomplished by performing Step (a) or Step (b).

- (a) From the TLTP (trunk and line test panel), access either TNN, operate the TWIN BUSY key, and then release the TRUNK key. Refer to AT&T Practice 231-050-009 for detail procedures.
- (b) At MTCE terminal, type the following message and observe TN06 CDFP 0 aaaaaa dddd LKDO output responses (where dddd = TG number).

T-TNN-TB 0 0 aaaaaa.

aaaaaa = TNN.

Use the MAKE BUSY key instead of the TWIN BUSY key, or use the T-TNN-LO or T-TNN-MB format of the above input message to remove just one trunk, of the pair, from service.

8.2.2 Restoring Trunks to Service

Trunks may be restored to service by performing Step (a) or Step (b).

- (a) If testing at the TLTP, release all necessary test keys, operate the RMV BUSY/REMOVE BUSY key for each trunk. Refer to AT&T Practice 231-050-009 for detail procedures.
- (b) If testing at MTCE terminal, type the following message for each TNN and observe TN06 CDFP 0 aaaaaa dddd ACT output response(s) (where dddd = TG number).

T-TNN-MA 0 0 aaaaaa.

aaaaaa = TNN.

8.3 Voice Diagnostics

The voice diagnostic test (Fig. 29) tests the relays of the CDFP OGT, verifies network continuity to the CDFP line appearance, and verifies the quality of voice as it passes through the CO-IVDM. This test may be requested by performing Step (1) or Step (2).

- (1) If testing at the TLTP, dial 6-digit TNN, then dial *00 and #. Refer to AT&T Practice 231-050-009 for detail procedures.
- (2) If testing at MTCE terminal, type one of the following:
 - (a) T-TNN-aa 0 0 tttttt.

ISS 1, AT&T 231-318-360

- (b) TRK-GROUP-aa 0 0 dddd.
- (c) TRK-LIST-fff.

aa = DG - Diagnose trunk (without a raw data printout)
 = DR - Diagnose trunk and print diagnostic raw data if a failure occurs (Not used in TRK-GROUP message). Refer to PK-1A045.
 = RT - Diagnose trunk 32 times and print failures (ATPs are not printed).
 ttttt = TNN
 dddd = TG number
 fff = DOS - Diagnose all trunks on the out-of-service list.

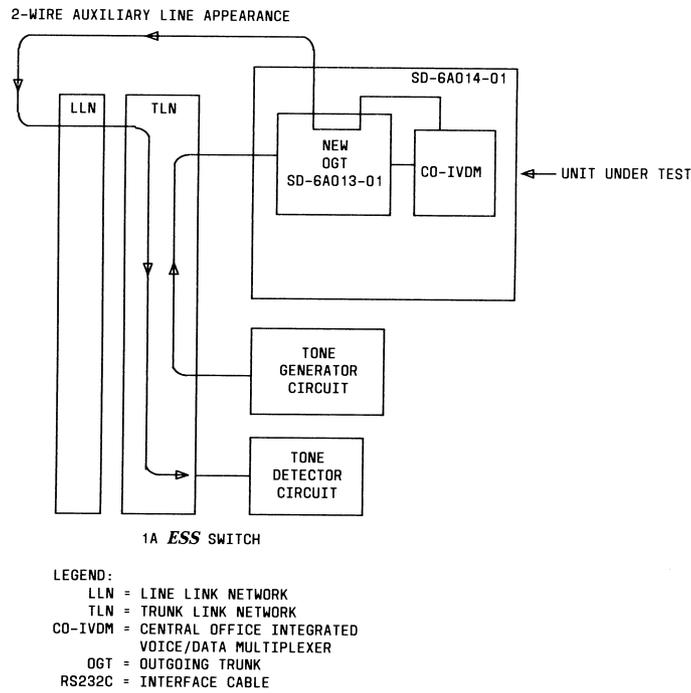


Fig. 29 — Voice Diagnostic Configuration

AT&T 231-318-360

In response to the above input, the system response should be TN01, TN05, or TN04 output message(s). Refer to OM-6A001 for interpretation of response.

If a trunk circuit fails (i.e., continuity check) during call setup or call disconnect, the trunk is placed on the TML (trunk maintenance list). Thus, the voice diagnostic is automatically requested.

Voice diagnostics can also be run at scheduled time intervals (APT). If a trunk circuit fails the diagnostic, the circuit is immediately retested. A second failure will result in the circuit being removed from service provided that the AML (automatic maintenance limit) for the TG is not exceeded. The AML for CDFP TGs is as follows: Not more than 1/4 of the first 16 trunks and 1/8 of the remaining trunks in a group can be removed from service.

8.4 Other Operational Trunk Tests

Other existing operational trunk test procedures can be used to test certain functions of the CDFP OGT from the trunk test panels (or via input messages). The functions that can be tested are listed below.

- 3-digit test codes - Display scan points
- 4-digit test codes - Operate and release relays.

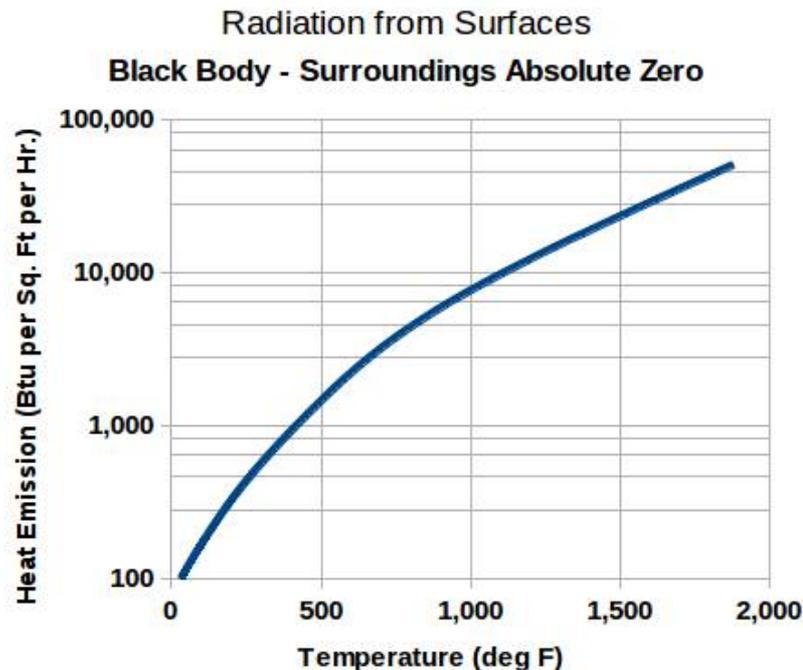
For details on the above test procedures, refer to AT&T Practice 231-050-009 (TLTP), AT&T Practice 231-050-008 (STTP), or AT&T Practice 231-050-007 (MTTP).

Techniques for Countering Thermal Imaging Devices

Introduction

Ever wanted to defeat those fancy thermal imaging devices the military and law enforcement agencies use? *Well...* You can't!

Every piece of matter in this universe above absolute zero (-459.69°F) emits radiation (in all directions) in the long-wavelength infrared band (2.5 – 25 micrometers) from its surface. This radiation is the result of the thermal agitation of the molecules which make up the matter. Basically, the hotter the mass – the more infrared energy it will emit.



From: www.engineeringtoolbox.com

FLIR Systems, the most common manufacturer of low-cost thermal imaging devices, use an uncooled Vanadium Oxide (VOx) microbolometer detector mounted behind a (germanium) filter which attenuates wavelengths below $7\ \mu\text{m}$. These VOx detectors are most sensitive to the $7 - 14\ \mu\text{m}$ wavelengths. You'll want to adapt your thermal camouflage to this particular wavelength range. It should be noted that natural atmospheric absorption effects wavelengths outside of the $3 - 5\ \mu\text{m}$ and $8 - 12\ \mu\text{m}$ "windows."

Emissivity is the measure of a material's ability to emit energy. It's an energy ratio referenced to a "black body" at the same temperature having an emissivity of 1.00 (the unit is arbitrary). All real-world objects will have an emissivity less than 1. In general, the duller and blacker a material is, the closer its emissivity is to 1. More reflective materials have a much lower emissivity. Aluminum foil has an emissivity of around 0.05, while black enamel paint has an emissivity of around 0.80.

Objects with a high emissivity and/or objects having a higher temperature relative to their background will appear as a silhouette when viewed with a thermal imaging device. The amount of contrast is relative to the emitted thermal radiation power of the object.

Reflectivity is the fraction of radiant energy that is reflected from a surface. Shiny, polished materials will have a high reflectivity, while matte or dull materials will have a low reflectivity. The emissivity plus reflectivity of a particular material should equal 1. That's to say, the more emissive a material is, the less reflective it will be.

The main techniques in "defeating" a thermal imaging device involve using low-emissivity materials on the exterior surface of your thermal-radiating object, or somehow reducing the exterior surface temperature so there is minimum contrast against the general background. And it's easier said than done...

For example, if you're in the middle of a grass field and cover yourself with an aluminized-mylar "space blanket" (which has a low emissivity, but a high reflectivity), you'll show up as a nice "cold spot" (it's blocking your body heat, but reflecting the cooler sky) against the general higher background thermal radiation from the surrounding foliage.

Thermal conductivity and equilibrium also means an object in close proximity to the thermal radiation source will also eventually "heat up." Preventing (or at least masking) this is the key to making ideal thermal camouflage.

Common Heat Radiation Emissivity Coefficients

Human Skin	0.98
Black Electrical Tape	0.97
Masking Tape	0.92
Water	0.95
Rubber	0.95
Glass	0.92
Plywood	0.83 - 0.98
Painted Surfaces	0.84 - 0.97 (non-aluminum)
Painted Aluminum	0.45
Black Paper	0.90
White Paper	0.68
Cardboard Box	0.81
PVC	0.91 - 0.93
Gravel	0.28
Grass	0.97
Fiberglass	0.75
Aluminum (polished)	0.05 (0.77 anodized)
Brass (polished)	0.03 (0.61 oxidized)
Copper (electroplated)	0.03
Cotton	0.77
Wool	0.78
Concrete	0.85
Nylon	0.85
Snow	0.82 - 0.85
Sand	0.76 - 0.95
Asphalt	0.93
Vegetation	0.80 (varies greatly)
Dry Soil	0.92
Wet Soil	0.95

* thermoworks.com/emissivity_table.html

* engineeringtoolbox.com/emissivity-coefficients-d_447.html

* www.infrared-thermography.com/material-1.htm

You'll note the low-emissivity materials tend to be shiny metals, which are not ideal for optical camouflage. They are usually sandwiched between an additional matte-colored isolating material to reduce their optical glare. You're essentially trying to match the emissivity and reflectivity of the general background to your thermal radiation.

Another example, skin has an emissivity of around 0.98. Covering it with some cotton fabric (emissivity of 0.77) would match your skin somewhat to a vegetation background of 0.80. But if the cotton fabric comes in direct contact with your skin, thermal conduction will also increase its temperature, causing it to radiate even more energy. Lining the interior of the cotton fabric with a thin metallic fabric layer would prevent your thermal radiation from heating the exterior cotton fabric.

Standard netting, or some other method of silhouette masking camouflage, should then be applied to the final outer layer. BTW, any thermal "contrast" movement will *STILL* be highly visible to a thermal imaging device.

I don't have access to a thermal imaging device for testing, but I do have some physics textbooks and Google. Here's some notes and observations I've come across during my research in anti-thermal techniques:

Anti-Thermal Notes & Observations



Intermat Anti-IR Thermal Skin Cream

Above is an anti-IR thermal skin cream from InterMat Defence Coatings (Greece).

It's a camouflage skin cream designed to be applied to your face, hands, or any other areas of exposed flesh, in order to attenuate your thermal radiation signature – while at the same time reflecting the surrounding background thermal radiation (to prevent contrast).

InterMat claims a person normally detected (via thermal imaging) at 1000 meters wouldn't be detected until 200 meters or so with their skin cream applied. Note that their skin cream appears to be quite shiny, so it may not be designed for daytime operations.

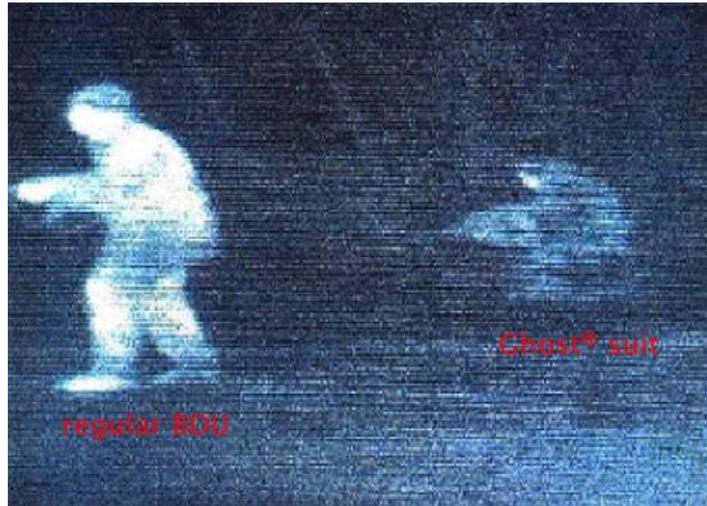
InterMat's skin cream formula is officially a "secret" and it's not sold to the taxpayers or voters (i.e. public), but I'm pretty sure it's just a very fine aluminum powder suspended in a jojoba oil / mango butter / beeswax consumer (non-fragrance) make-up base.

You'd probably have to experiment a bit to get the right consistency. I know absolutely nothing about homebrew make-up (or chemistry), but this seems like it would be a good starting point for your own version...

The binder material holding the aluminum powder in your homebrew anti-thermal skin cream (or paint) should *NOT* have a strong absorption in the thermal radiation band (7 – 14 μm) to prevent creating thermal "holes." Other low-emissive metal powders should also work, but aluminum powder tends to be the cheapest and easiest to find – and it probably won't kill you.

(intermatstealth.com)

(defensereview.com/intermat-anti-thermalir-camo-tech-for-infantry-and-special-operations-forces)



Above is an example of an infantryman wearing Ghost thermal camouflage fabric from Blucher Systems (Germany).

Blucher System uses a fabric which incorporates metallized fibers and is available in various visual camouflage prints. They claim significant signature reduction in the ultraviolet (0.2 – 0.4 μm), near-infrared (0.7 – 2.5 μm), and thermal-infrared (3–5 μm / 8–12 μm) ranges.

Blucher does, however, sell a version of this fabric to the public which attenuates everything except the thermal-infrared band (i.e., it's missing the metallized fiber liner).

Note that most modern military Battle Dress Uniforms (BDUs) contain an "anti-IR" fabric, but this material is designed for attenuating the near-infrared band which most standard image intensifier night vision devices (and active infrared illuminators) operate at.

Many artificial fabric materials tend to strongly reflect radiation in the near-infrared band. Keep this in mind if you ever want to create your own "Camo Dude Detector."

Washing these BDUs with a consumer detergent containing "optical brighteners," or other detergent containing starch, will gradually weaken the anti-IR coating. Using Woolite is fine.

The above picture is also a good example of why it's so difficult to defeat infrared motion sensors which operate in the same thermal-infrared band.

Even if you *completely* block your thermal radiation signature, the contrast against the "warmer" background via your motion may still set off the sensor.

Most infrared motion sensors use dual infrared detectors arranged in a differential configuration. Slowly raising the overall temperature of the general target area won't set off the alarm, but any contrasting thermal radiation passing across the infrared detector will create a "difference pulse," triggering the alarm.

(eng.bluechersystems.com/produkte/C10)

(youtube.com/watch?v=nx0ggSL8CkU)



Above is a real-world thermal imaging example (left) of the April 15, 2013 Boston Marathon bombing suspect.

The Obama supporter hid in a boat which appears to have some type of protective plastic cover or tarp.

As you can see, the thin plastic cover has a high emissivity / low reflectivity, and is fairly transparent to longer wavelength thermal radiation. Hence, the thermal radiation from his body can pass right through the boat cover. That's his outline in black in the left picture.

If the boat cover had been lined with a low-emissive material, like aluminum, his thermal radiation would have been reflected internally (and dissipated) within the boat's interior and he may not have been noticed from the overhead FLIR-equipped helicopter.

Also note, in the left picture, how the boat itself contrasts against the general grass background – you can even clearly see a ladder near the trailer's tires.

Those objects are not emitting a great amount of thermal radiation, but their emissivity is different from the general background, causing them to stand out.



"Anti-drone hoodie" by Adam Harvey.

While more of an art project than a piece of tactical gear, his overall concept is quite sound.

A metallic fabric is combined with a silk liner to produce a "flowing" anti-thermal fabric. The silk liner also helps a little to isolate the hoodie from your body to reduce thermal conduction.

Note how the person wearing the hoodie appears as a "thermal hole" in the above picture. This would need to be combined with some other type of visual camouflage to breakup the distinct outline of a human.

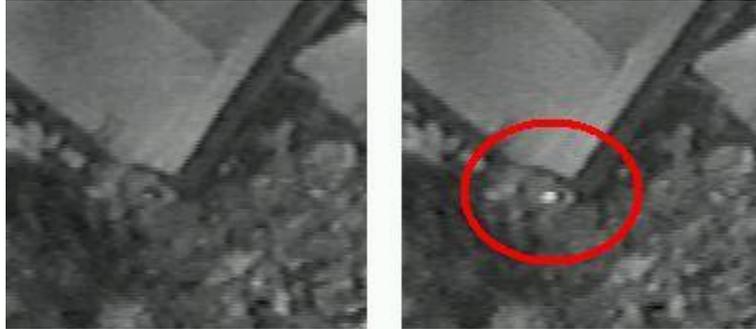
A person wearing this anti-thermal hoodie within a group of people *not* wearing similar hoodies would stand out just the same as if they were in the middle of a field. This emphasises the need to monitoring your thermal contrast when trying to avoid a thermal detection device.

I'm pretty sure the metallic fabric is similar to that which was used in the anti-TASER experiments in *GBPPR 'Zine*, Issue #42.

The fabric can be purchased from LessEMF, though it's still quite expensive, around \$20 per linear foot.

(ahprojects.com/projects/stealth-wear)

(www.lessemf.com)



Knowing what you know now, review the overhead FLIR video footage from the 1993 Waco compound massacre.

You'll notice a number of thermal "flashes" coming from the bushes, and other concealed areas, surrounding the compound after it was set on fire. (The tear gas used a flammable propellant.)

Remember, thermal imaging devices contain a high-pass filter which severely attenuates the normal visible light spectrum. Those "flashes" had to contain energy in the thermal-infrared band.

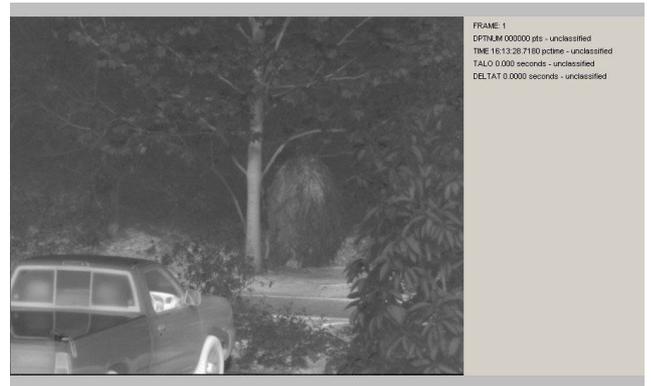
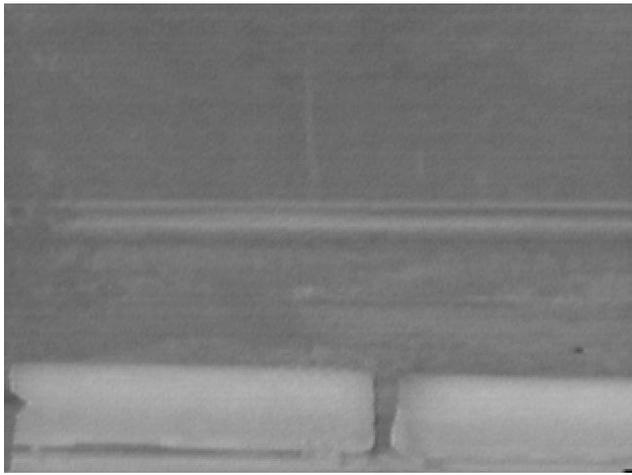
The flashes are most likely gunshots from FBI snipers shooting at innocent people trying to flee a building the government just set on fire.

The official U.S. government report on the Waco massacre says there wasn't any sniper fire...

Check out *The FLIR Project* by Michael McNulty for more information on the Waco coverup.



A sniper who officially didn't exist.



Example thermal imaging pictures of a man wearing a Custom Concealment, Inc. Thermal Ghillie Suit.

Their anti-thermal ghillie suits are not available to the public, but it's most likely just a regular ghillie suit with an internal liner of metallic fabric and another wool/cotton/silk/etc. insulating layer to keep it away from your body.

(www.ghillie.com/thermal.htm)

Additional Notes on Thermal Camouflage

1. Due to the high internal reflection nature of germanium-based lenses, it is possible to "jam" a thermal imaging device by overpowering the optics with a carbon dioxide laser operating at the 9.4 or 10.6 μm wavelength. This is how some types of "anti-missile lasers" on commercial/military airplanes work. They are essentially overpowering the heat-seeking optics in the missile's guidance system. Actually directing a narrow-diameter laser beam onto the (potentially moving) missile optics will be an exercise left for the reader!
2. Adding a layer of microwave ferrite absorption material, like Eccosorb, to your camouflage will attenuate microwave radiation used for some motion alarms and overhead synthetic aperture radar systems.
3. Gila Films (gilafilms.com) sells a "heat control window film" which you should be able to find at your local hardware store. It comes in 2 x 15 foot rolls and is designed to improve the thermal performance of older house windows by reflecting sunlight, trapping internal thermal energy, and reducing ultraviolet radiation. It attaches to the window's surface using a soapy water solution and a squeegee.
4. The resolution on some modern military-grade thermal imaging devices is high enough to identify faces based solely on their "heat" signature.
5. Damp, raining, dense fog, or other wet environments offer the best natural protection against thermal boundary contrasts.

Battlefield Laser Warning Receiver

Introduction

"In the far distance a helicopter skimmed down between the roofs, hovered for an instant like a blue bottle, and darted away again with a curving flight. It was the Police Patrol, snooping into people's windows. The patrols did not matter, however. Only the Thought Police mattered." --- Quote from George Orwell's *1984*.

Barack Hussein Obama, Jr. is a fraud. A Kenyan-born Marxist Muslim usurper. A creation of the liberal media. A puppet for a handful of international central bankers and the 1%.

He's kept aloft by a continually dumbed-down public (to keep them voting Democrat), blindly ruled by oligarchs. Surrounded by his gang of anti-American extremists and tyrants who wish to control your every thought and move.

Steal \$1.2 billion from MF Global and you can run the Obama re-election campaign. "Steal" a bunch of taxpayer-funded academic papers and you'll have your entire life ruined. You don't need to show an ID to vote to start a war, but need a full interrogation to fly on a plane or to enact your God-given right to own a gun. Change!

As the traitorous Goldman Sachs/General Electric/Chicago Mafia Obama regime continues to turn the United States into a nation of takers instead of a nation of makers, expect to see more violent extremism and corruption, the endless printing of funny money to keep the public docile, and racially-motivated attacks against his political enemies – all in order to take the public's mind off his failed policies and your loss of freedom.

Their latest tool is using unmanned Predator/Reaper drones equipped with laser-guided AGM-114 Hellfire missiles to kill people – including Americans – without any type of due process or jury trial. Change!

Most U.S/NATO/ZOG laser-guided bombs and missiles use a diode-pumped, Q-switched (pulsed) Neodymium-doped Yttrium Aluminum Garnet (Nd:YAG) laser designator operating at a 1064 nanometer (+/- 2 nm) wavelength. The designator's optics will have a low divergence, with most under 300 microradians. That means the laser beam's effective area is about 1 meter square (or smaller) at a range of 3 kilometers.

The laser's pulse width is around 15 to 25 nanoseconds with the pulse energy around 50 to 120 millijoules. The use of very narrow pulses means the peak output optical power is actually several thousand watts. The laser's Pulse Repetition Frequency (PRF) is usually between 8 to 20 Hz (+/- 1 μ S pulse resolution) and is externally selectable.

An individual PRF "code" is what is programmed into the bomb/missile seeker and laser designator ahead of time. The codes are three modified-octal digits (111-488 [Band 2] and 511-788 [Band 1]), but some codes are four digits and should always start with a "1" (1111-1788). There are a total of 677 different codes. The code numbers determine the pulse rate, and the faster pulses are easier for the missile's laser seeker to lock-on to in a cluttered environment. Each weapon system is assigned its own laser code to prevent interference with other systems. NATO designator codes are officially listed in STANAG 3733, which is not available to the public.

I believe the codes may be directly related to the PRF or the somehow related to the timing between the laser pulses. For example, code 1234 would have a 12.34 Hz PRF. A confirmed operational (Apache-launched) Hellfire missile laser code is 1155. Overhead Predators can "lase" targets for the Apaches, if so needed.

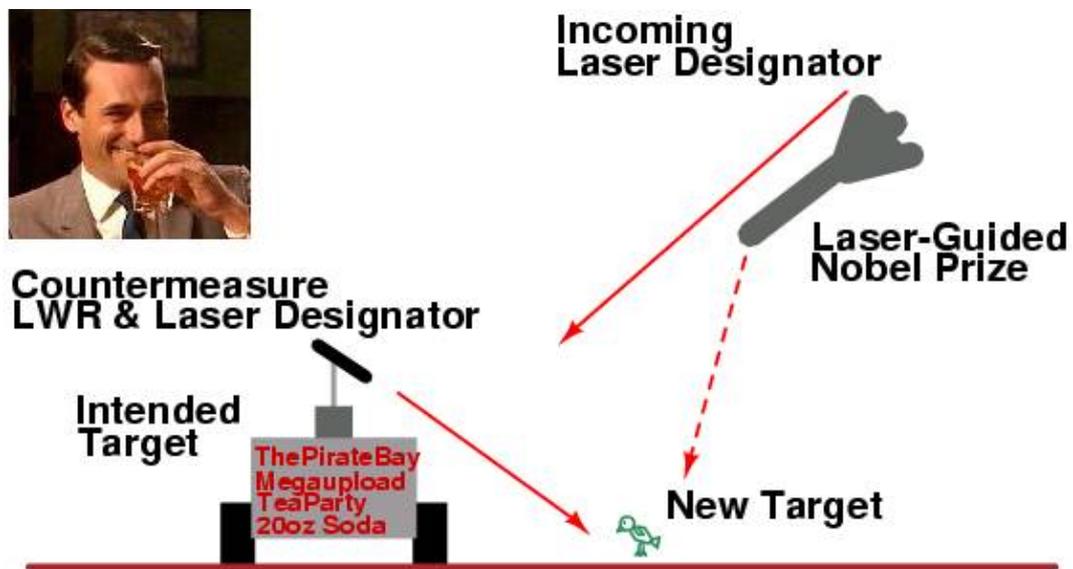
The laser designator illuminates the intended target and the bomb/missile seeker "flies" into the reflected energy. There can be up to 30 seconds from the time the laser is activated to the impact of the bomb/missile. The laser designator and the bomb/missile seeker head need to both be pointing towards the target before launch. A laser "back scatter" condition can exist where sand/dust/etc. in the air causes a false lock before the bomb/missile is launched.

The Hellfire missile has an indirect launch mode called "lock-on after launch" in which the missile is initially launched in an unguided mode, then seeks out the laser reflection while in the air. This is a countermeasure to minimize the amount of time the laser designator needs to be activated. The maximum range of the Hellfire is around 8 km.

Another potential countermeasure is called "offset designating," where the laser is aimed at a location near the target but just far enough away not to trigger a laser warning alarm.

If you're a troublemaker, it should be possible to detect the activation of an enemy laser designator, then generate *YOUR OWN* laser pulses at the same PRF. You'd then point your high-power laser at a nearby location to "distract" the incoming bomb/missile from its intended target.

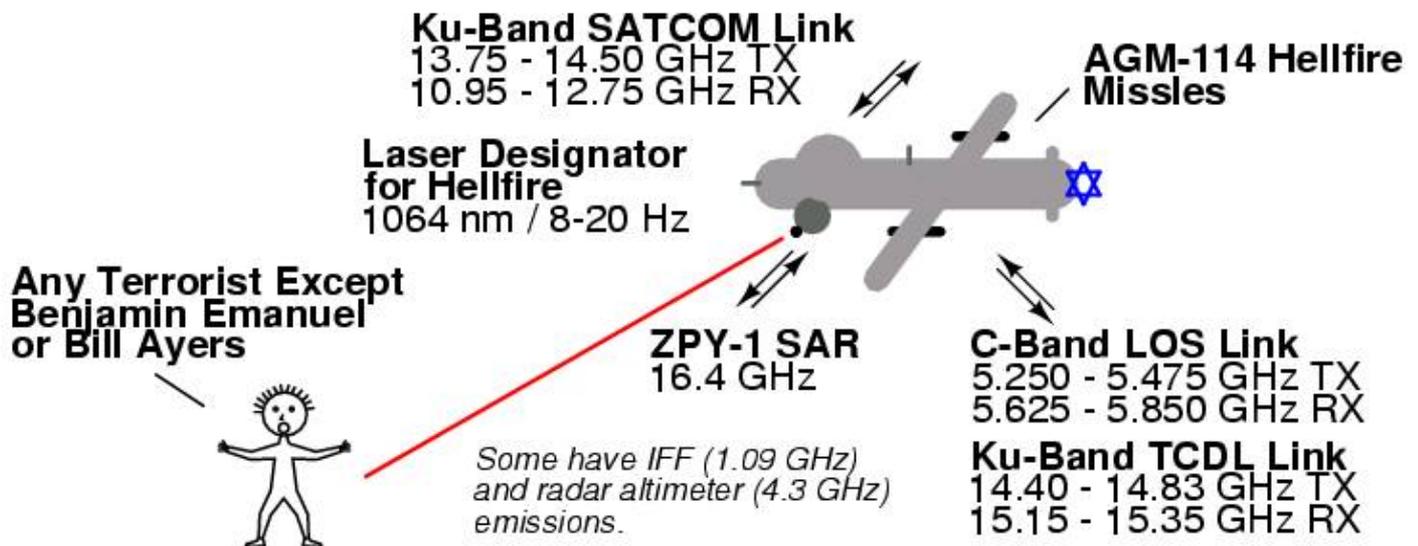
Note that the seeker PRF codes are often transmitted over the various open radio channels (or standardized) and some laser-based professional tattoo/hair removal systems use the same type of pulsed Nd:YAG laser...



Many UAVs can be located and tracked via their optical, acoustic, and radio emissions. Directional microwave and satellite wireless links combined with spread-spectrum modulation is making this increasingly difficult for the undocumented SIGINT interceptor, but you'll be surprised what's out there.

Yes, some UAVs use commercial satellite relays when not operating in a "line-of-sight" mode. eBay has all sorts of high-power Ku-band uplink transmitters and amplifiers you can use to jam, *err...* "simulate noise" on those particular satellite channels.

General Atomics MQ-1 Predator



Overview

This Battlefield Laser Warning Receiver (LWR) project is a *very experimental* design to try and detect the pulses emitted from an enemy laser designator. The circuit will use mostly off-the-shelf components to reduce cost and to simplify the construction.

While searching through patents for "laser warning receiver," I came across U.S. Patent 5,260,563 by Tracor Aerospace. This patent appears to be for their portable LADIS (Laser Alarm for the Individual Soldier) battlefield laser warning system. A few components in their schematic are unlabeled, but can be determined via the detailed description of the circuit's operation in the patent text.

This LWR project will be based on the stock Tracor schematic, but with a few minor changes. You'll want to print out the patent, then read and re-read the entire text before constructing this circuit to get an idea of what's going on. A different front-end PIN photodiode pre-amplifier circuit will be constructed as I was unable to get the circuit in the Tracor patent to operate properly.

The main optical sensor will be three Vishay BPW34 silicon PIN photodiodes in parallel. These are not the ideal photodiodes for detecting a high-speed laser pulses at 1064 nm, but they're cheap (around \$1 at Digi-Key) and they're also listed in the Tracor patent. InGaAs PIN photodiodes salvaged from high-speed fiber optic connections will provide a *much* better response at 1064 nm, but silicon PIN photodiodes will still work for experimenting.

This should still be considered a test circuit to get a general idea of what it takes to detect a high-speed laser pulse. An "ideal" battlefield LWR would have multiple optical sensors (and log amps) to cover the full 360°, plus a couple pointing up for aerial coverage. Combined, these could also provide bearing data back to the enemy designator.

The original Tracor design has a simple Automatic Gain Control (AGC) circuit to help discriminate against background light pollution or sunlight, but optical (infrared) bandpass filtering the incoming signal is still recommended.

Because of the LWR circuit is intended to detect very fast rise-time laser pulses, the front-end amplifier(s) should be designed with a fairly wide RF bandwidth (100+ MHz) in mind. Proper RF circuit constructing techniques, such as a large ground plane, surface mount components, RF shielding, and proper DC power supply decoupling, should be followed to prevent the circuit from oscillating or amplifier degradation.

The three parallel BPW34 PIN photodiodes (making up a single array) will have a reverse bias voltage (+10 VDC) on them to help increase their detection bandwidth. A 2N4416A JFET provides a very high impedance buffer between the PIN photodiodes and the next stage amplifier.

The signal pulse from the 2N4416A is amplified by a Motorola MWA120 Wideband General-Purpose Hybrid Amplifier. The MWA120 has a fixed gain of around 14 dB from DC to over 400 MHz and a standard 50 ohm input/output impedance. The MWA120 probably isn't the ideal amplifier, but I had a couple laying around and they require a minimum of supporting components. The detected laser designator pulses should be fairly strong, so not alot of gain is required. Wideband video amplifier ICs like the National LM733 should also work.

The output from the MWA120 is sent to a Motorola MC13055 Wideband FSK Receiver to generate a logarithmic output voltage based on the input power of the signal pulse. The MC13055 has around 70 dB of input power detection range (-80 to -10 dBm). The higher the power of the pulse is, the higher the voltage output will be. The Tracor circuit uses a Motorola MC13055, but the Motorola MC3356 should also work and may be a little easier to find.

The logarithmic voltage output from the MC13055 is then sent to a LM311-based comparator circuit. When the output pulse voltage reaches a preset threshold setting determined by a panel-mount 20 kohm potentiometer, the LM311's output goes high. The LM311's output can be used directly as a "digital" logic level (10 volt) signal, or to trigger a 555-timer in a monostable "pulse stretcher" operation. The 555 can then light a warning LED or signal an audio buzzer as the final laser warning alarm.



AGM-114 Hellfire on a Predator Drone

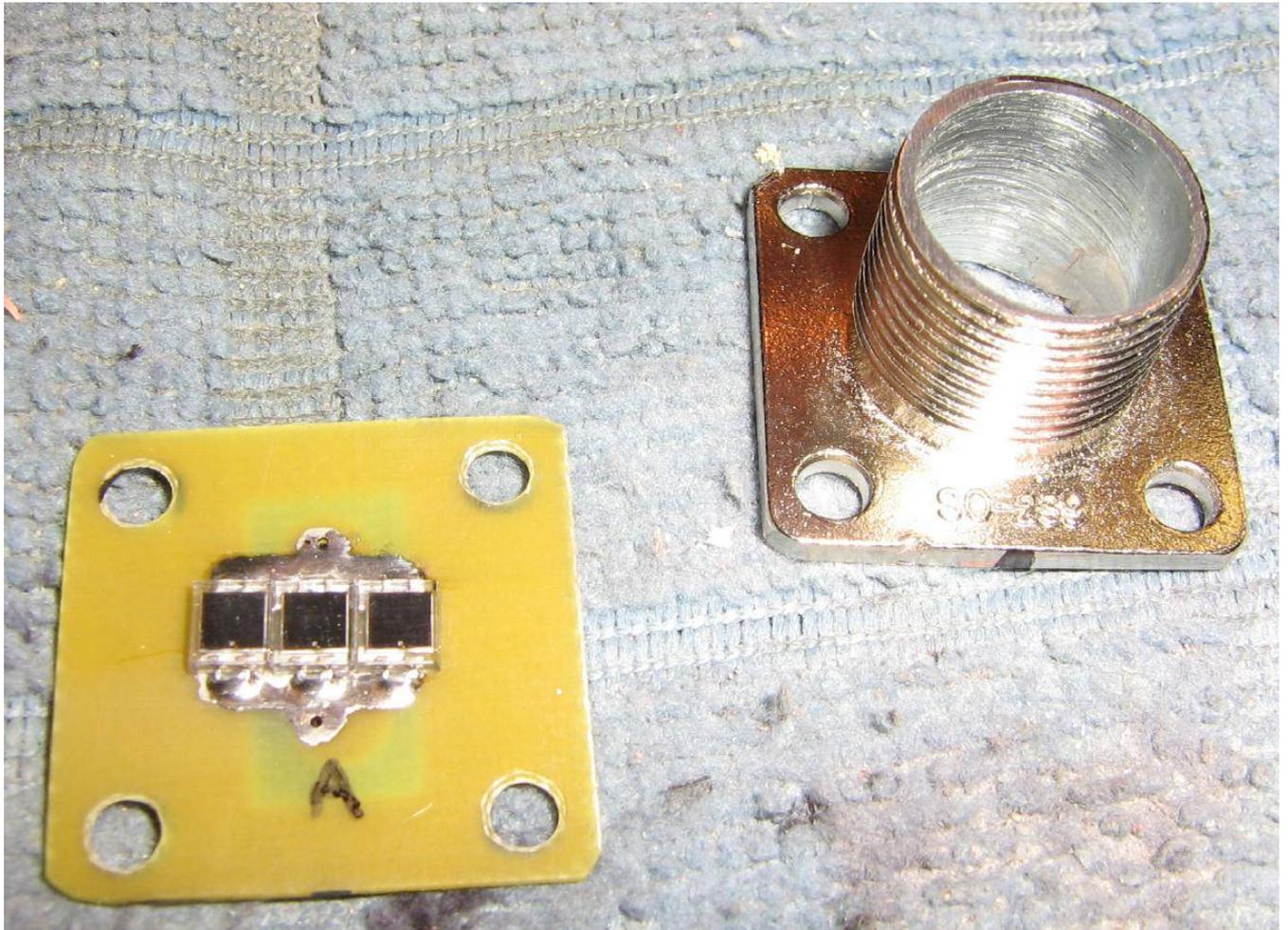
Pictures & Construction Notes



Overview of the parts for a single BPW34 PIN photodiode array for the Battlefield Laser Warning Receiver.

Three surface-mount Vishay VBPW34S PIN photodiodes are arranged in parallel and mounted behind a SO-239 connector which has had its internals removed.

The coupling ring is from an old CB radio microphone connector. It uses the same threads as the SO-239 and will be used to hold an optional infrared bandpass filter.



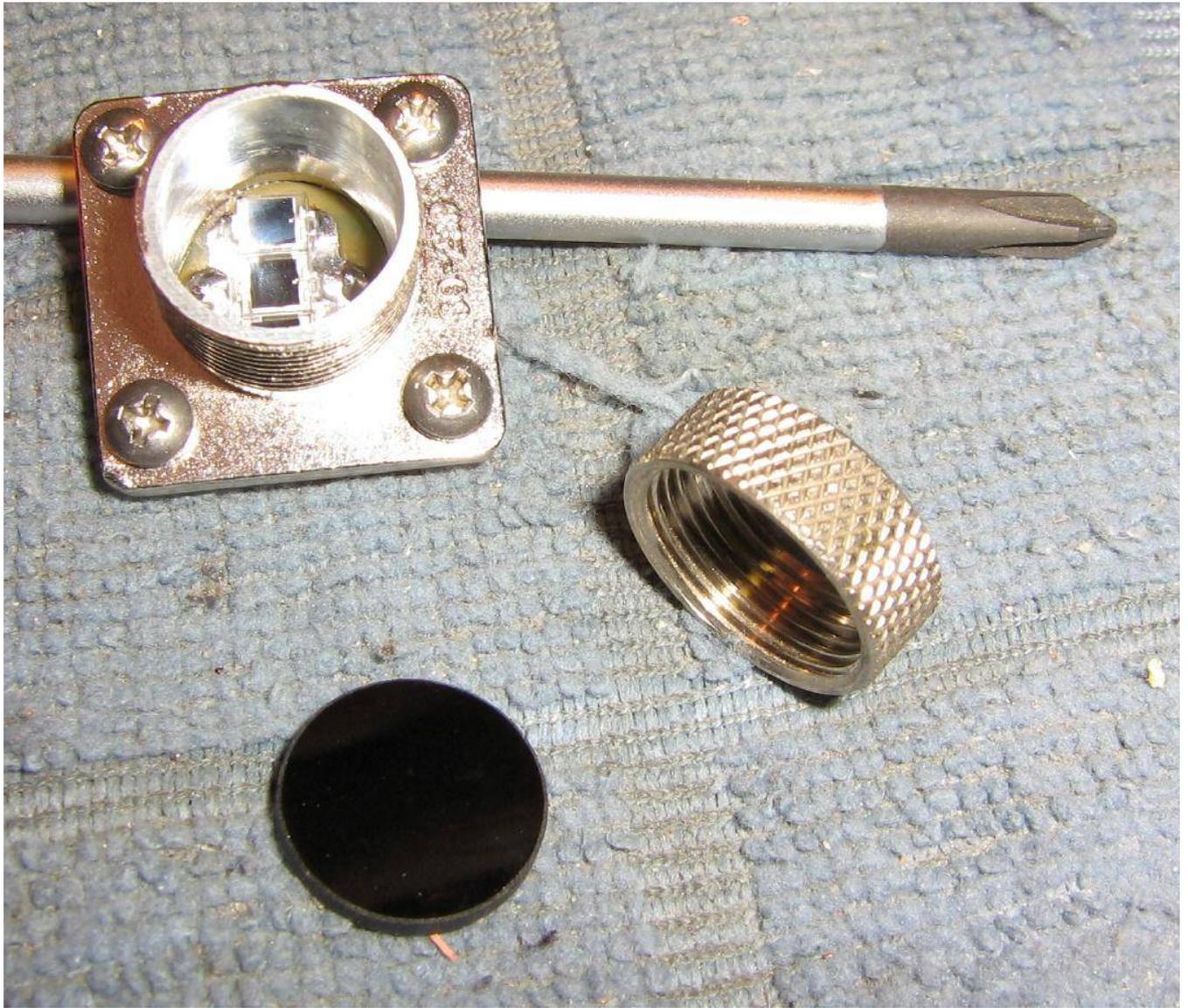
Closeup view of the three parallel BPW34 PIN photodiodes mounted onto a little circuit board with matching holes for the SO-239 connector.

The drilled out (1/2-inch) SO-239 connector is on the right.



Attaching the BPW34 PIN photodiode circuit board to the rear of the SO-239 connector.

The inside of the SO-239 connector should be painted flat black to prevent off-axis reflections.



Shown with the optional infrared bandpass (808 – 1064 nm) filter.

These filters are available on eBay for around \$10.

The 15 mm diameter filter fits the coupling ring perfectly.

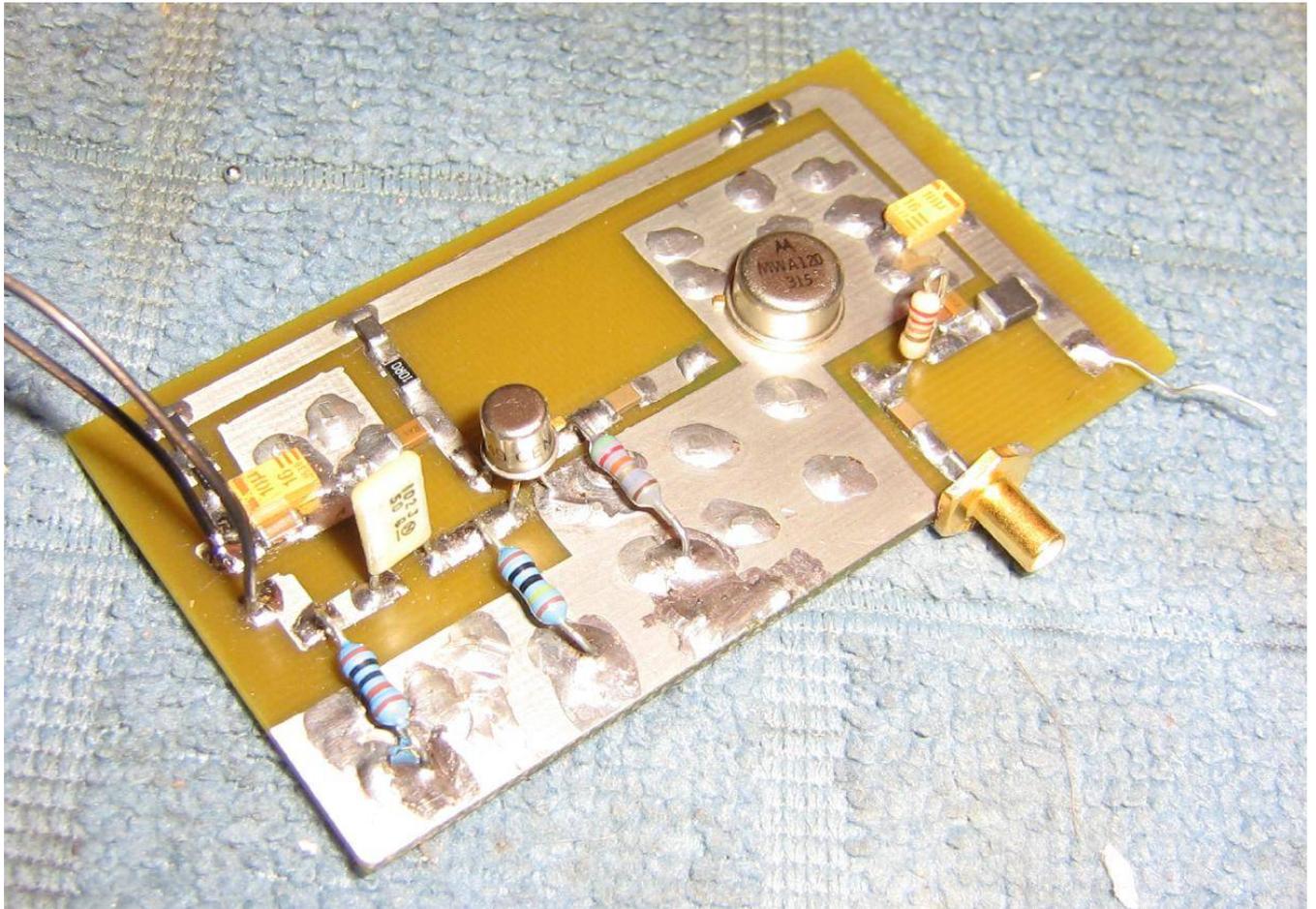
Search eBay for something like "Filter Color Glass Lens against 400nm–750nm through IR Infrared 808nm–1064nm."

Really...



Completed single PIN photodiode sensor array for the Battlefield Laser Warning Receiver.

For a real-world application, multiple PIN photodiode sensors should be used and arranged for 360° coverage, as well as a few for aerial coverage.



Overview of the front-end amplifier circuit for the PIN photodiode array.

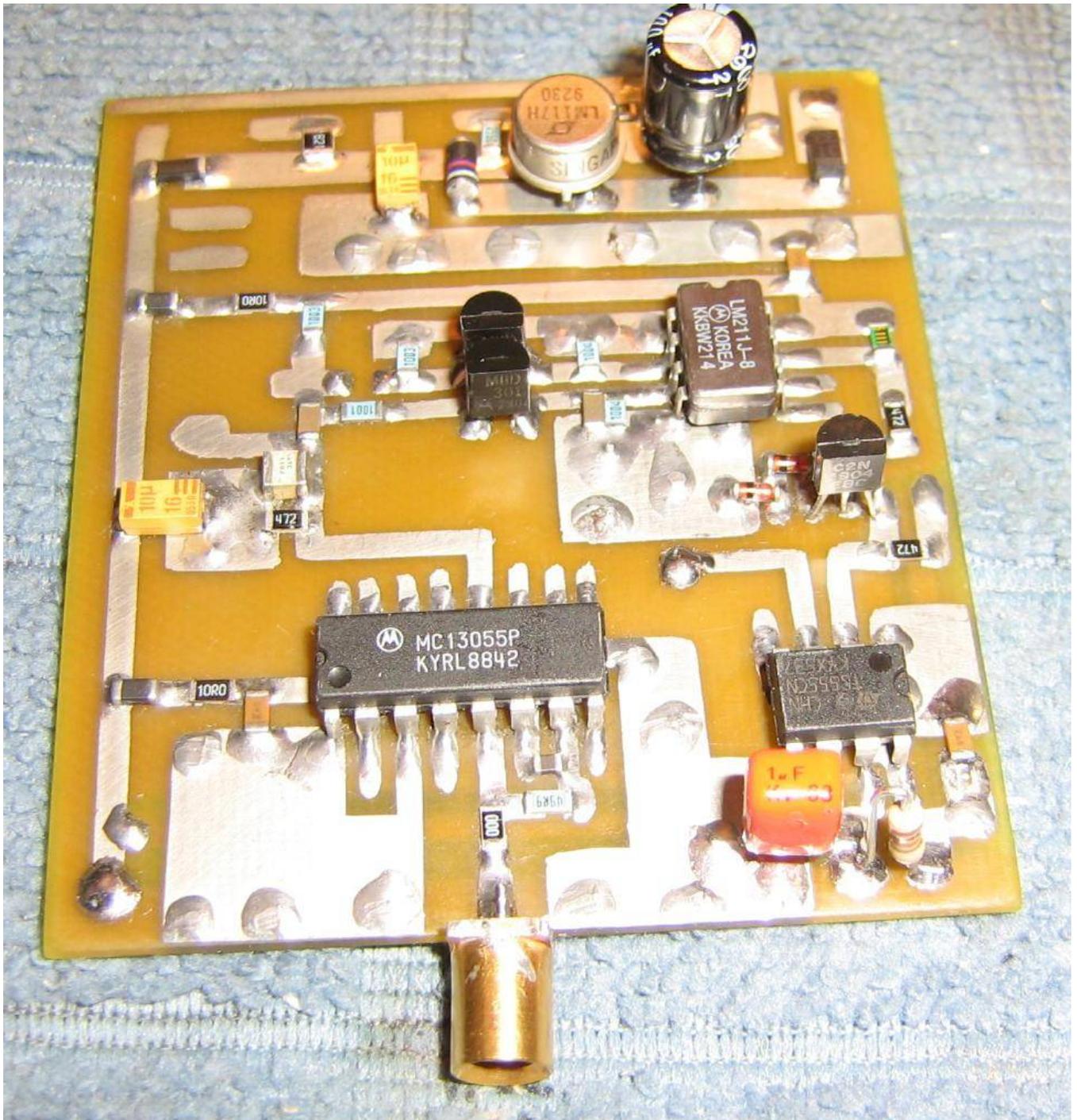
The small-canned item is the 2N4416A JFET buffer.

The large-canned item is the MWA120 amplifier.

This board is powered from an external +10 VDC source.

The front-end amplifier is on a separate circuit board (and uses leaded components) due to continuous experimentation.

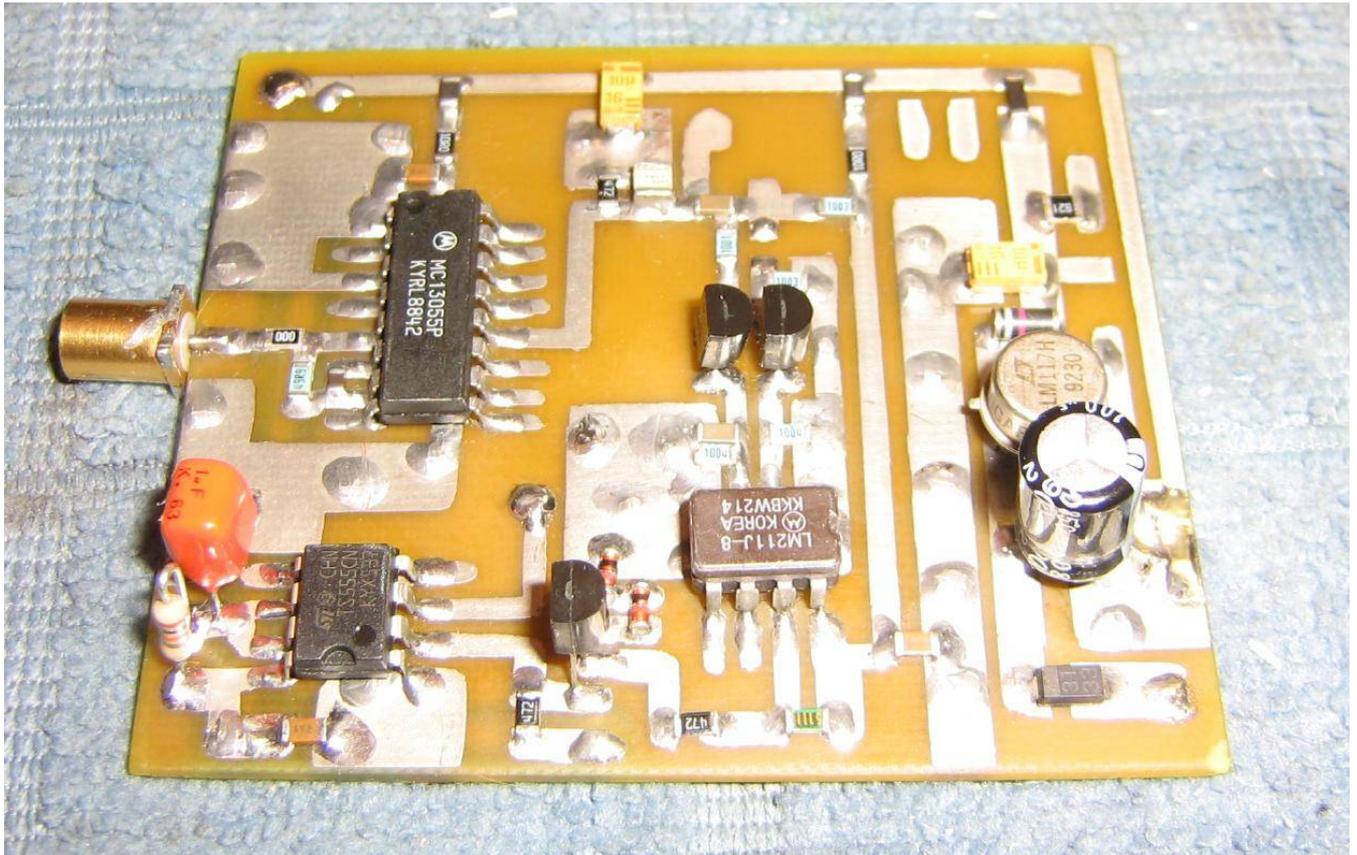
An ideal front-end amplifier circuit should have a little more gain and include some type of automatic gain control.



Overview of the logarithmic amplifier, comparator, and alarm generating circuit.

This circuit has been pretty well debugged and should work as-is. It's based around the logarithmic amplifier and comparator circuit in the Tracor patent.

A LM117 voltage regulator is along the top. This generates a clean source of +10 VDC for the circuits from a +12 VDC input. The current draw is minimal.



Alternate view of the logarithmic amplifier, comparator, and alarm generating circuit.

The +12 VDC power comes in on the lower-right.

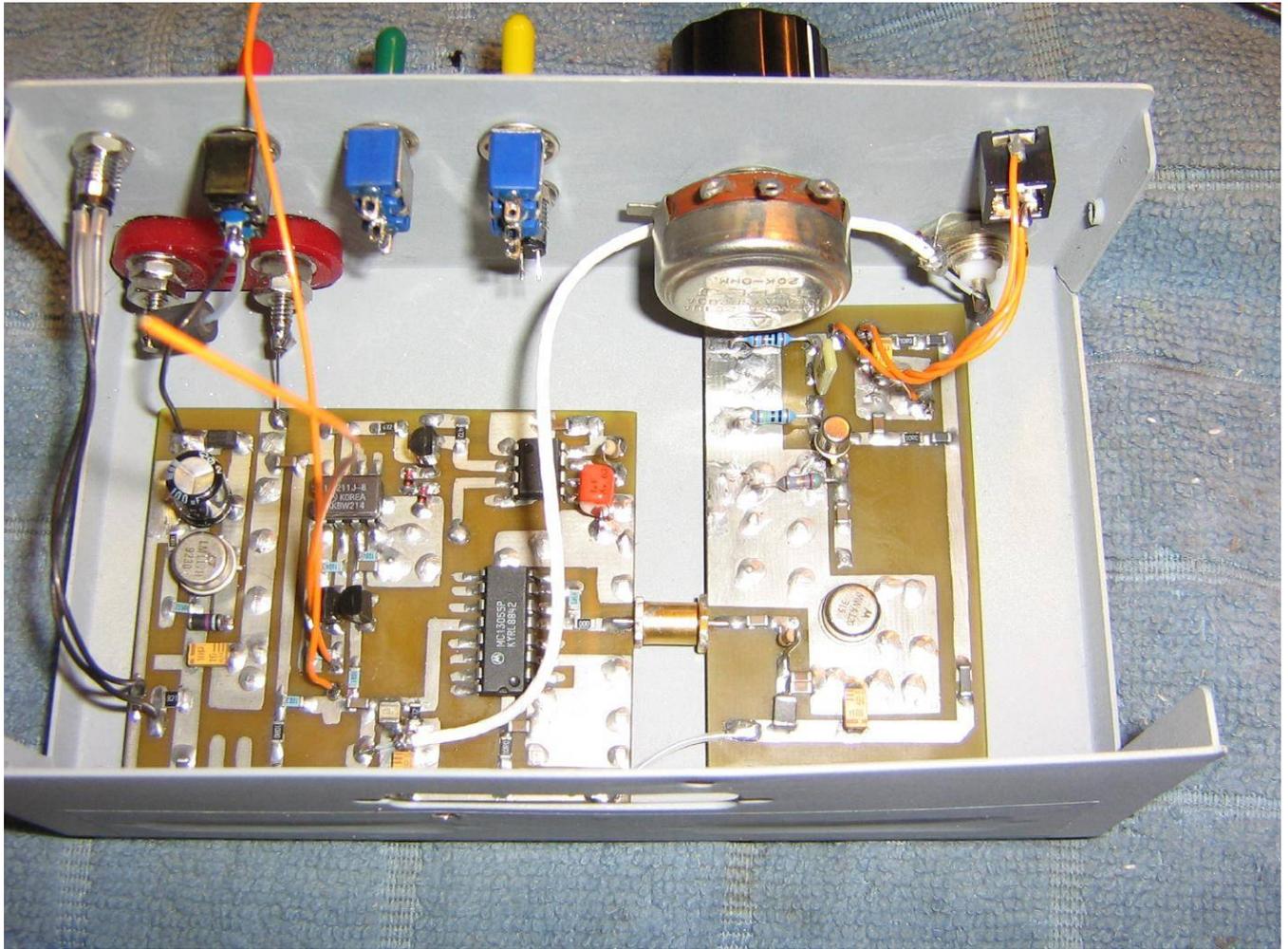
The 16-pin IC is the MC13055 logarithmic amplifier. The 555 pulse stretcher circuit is below it.

The two items in the middle which look like transistors are the MBD301 Schottky diodes for the LM311 comparator circuit. A LM211 is used in place of the LM311 in this example.

When a proper "pulse" is detected by exceeding an externally settable threshold on the LM311 comparator circuit, it toggles a transistor which in turn activates the 555 pulse stretcher (monostable) circuit. The large orange 1 μ F capacitor is part of the 555's timing circuit.

The 555 timer essentially turns the incoming nanosecond pulses into 10 millisecond long pulses.

These longer pulses are used to directly sound a buzzer or light a LED to act as a final warning alarm.



Completed circuit, internal overview.

Mounting the circuit boards in an old printer switch case.

+12 VDC power input is via the banana jacks on the upper-left. A power-indicating red LED and power switch are above it.

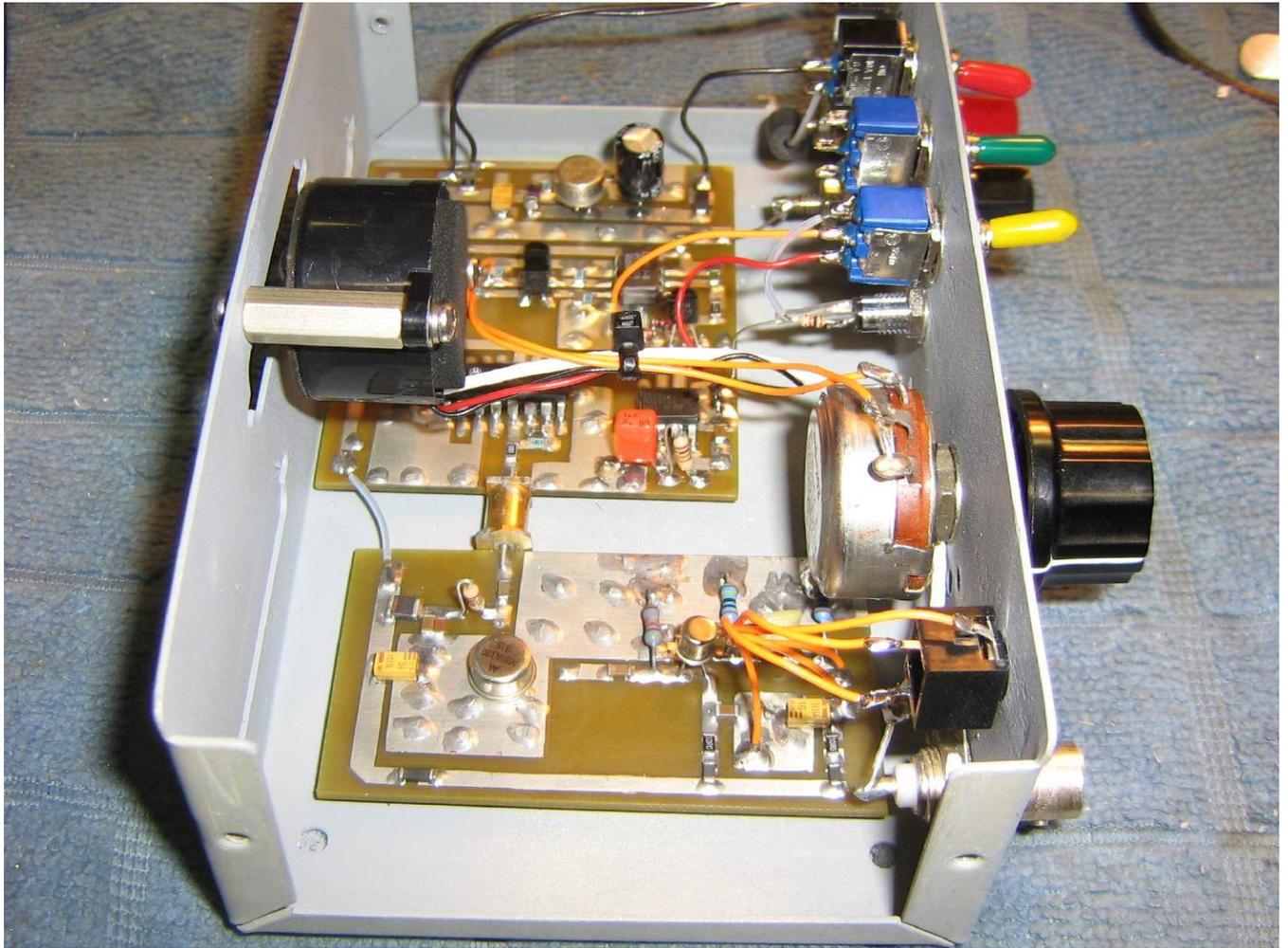
The green toggle switch isn't used at this time.

The yellow **Alarm Select** toggle switch chooses either a buzzer or LED warning alarm.

The 20 kohm potentiometer sets the threshold in the pulse comparator circuit.

A 1/8-inch stereo jack is used to connect to the external PIN photodiode array. Be sure to use shielded wire. The tip should be the cathode, ring the anode, and sleeve the ground.

A front-panel mounted BNC jack is used to directly monitor the MC13055 logarithmic output voltage. This output can also be used for further signal processing. A small piece of coax should connect this output to the front-panel BNC jack.



Alternate interior overview.

A warning alarm buzzer has been added. This is selectable via a switch on the front-panel.

The buzzer should have its own internal driver circuit and should also be capable of being driven directly from a 555 timer. If it can't, an additional transistor driver should be used. Radio Shack carries a couple of suitable buzzers.

The buzzer will sound in unison with the detection of the incoming pulses. For example, if the laser designator PRF is 12 Hz, the buzzer will also sound 12 times a second at 10 millisecond intervals.



Completed Battlefield Laser Warning Receiver.

The logarithmic amplifier **Monitor** BNC jack is on the lower-left.

The **PIN Input** 1/8-inch stereo jack is mounted above it.

The 20 kohm **Threshold** potentiometer is in the middle.

The green laser warning LED is below the **Alarm Select** switch.

To use the unit, connect the PIN photodiode array via a standard shielded stereo cable with a 1/8-inch plug (tip: cathode, ring: anode, sleeve: ground).

Turn the **Threshold** control completely counter-clockwise.

Apply +12 VDC power to the unit and turn it on.

The buzzer should sound or the LED should light, depending on the **Alarm Select** switch setting.

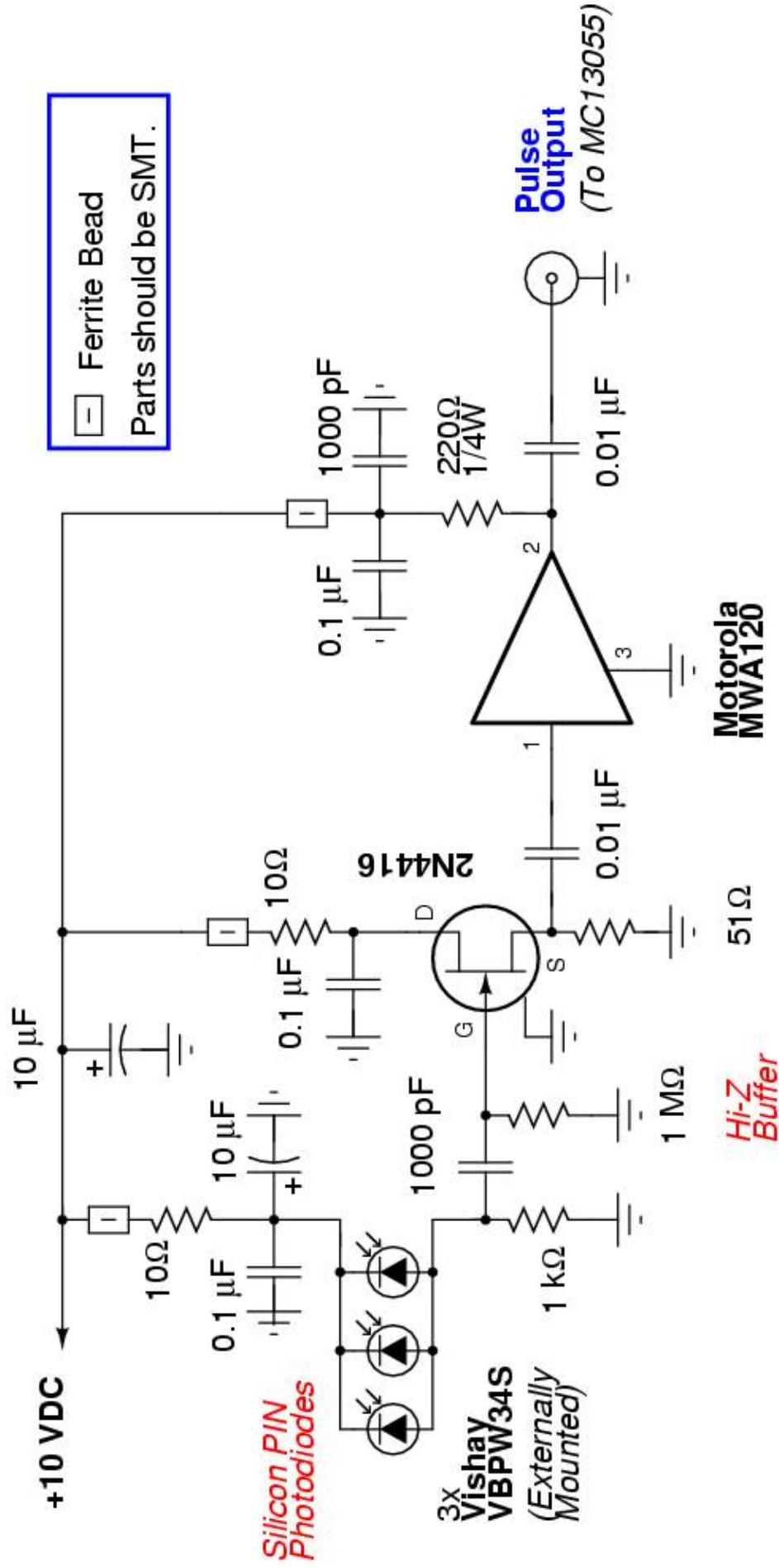
Slowly rotate the **Threshold** control clockwise until the buzzer/LED stops.

This sets the minimum pulse threshold for that particular environment. The **Threshold** control may need to be continually adjusted to match other lighting conditions.

To test the LWR, set the **Alarm Select** switch to buzzer, then point a standard TV remote control at the PIN photodiode array. Pressing any buttons on the remote should cause the buzzer to sound.

Battlefield Laser Warning Receiver

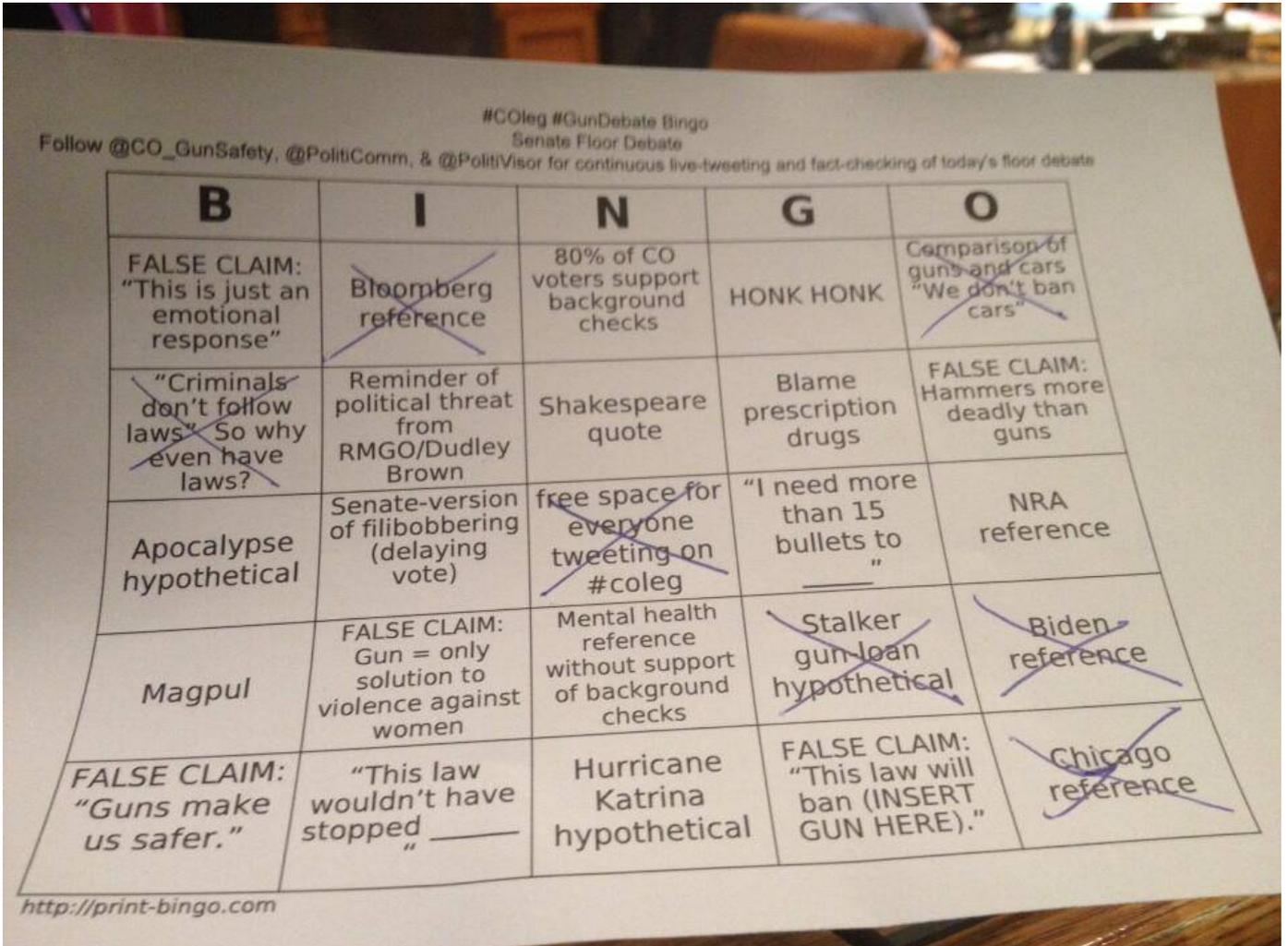
Front-End Amplifier



Hi-Z Buffer

Pulse Amplifier

Bonus



Anti-gun tweet by an Associated Press "reporter."

While covering the Colorado State Senate debates over their sweeping gun control legislation on March 8, 2013, Colorado-based Associated Press political reporter Ivan Moreno took time out to tweet an "awesome" and wildly anti-gun bingo sheet.

(theblaze.com/stories/2013/03/08/did-an-ap-reporter-let-his-anti-gun-bias-show-check-out-the-gun-control-bingo-sheet-he-called-awesome)

(twitter.com/IvanJourn/status/310138341746155520/photo/1)

End of Issue #109



Any Questions?

Editorial and Rants

Wow, a public school teacher actually trying to do the right thing – too bad it was in Obama's Chicago! We'd all be considered "terrorists" based on the stuff we brought to school (pocket knives + ham radios & scanners) in my day. It's just a matter of time before they start banning pens and pencils. Wouldn't want any original thoughts or critical thinking now, would we?

Political Correctness Run Amok at School

April 17, 2013 – From: courthousenews.com

by Courthouse News Service

CHICAGO (CN) – A Chicago public school suspended a teacher without pay for showing his students a little pocket knife, "as part of a curriculum–mandated 'tool discussion,'" the teacher claims in court.

Douglas Bartlett sued the Chicago School District No. 299 and his principal, Valeria Newell, in Federal Court.

Bartlett was a second–grade teacher at Washington Irving Elementary School, on Chicago's South Side, when he was suspended, in the 2011–12 school year. He was in his 17th year with the school district.

"This is a suit for violation for plaintiff's constitutional due process rights resulting from the overzealous application of political correctness," the complaint states. "Plaintiff, a school teacher, showed to his students a pocket knife, as part of a curriculum–mandated 'tool discussion.' Other garden–variety tools plaintiff used in the discussion were a box cutter, various wrenches, screwdrivers, and pliers. As a result of showing a pocket knife, plaintiff was charged with bringing a weapon to school, and received a four–day suspension without pay. Plaintiff sues for money damages and to have this suspension expunged from his record. Plaintiff seeks relief pursuant to 42 U.S.C. § 1983 for redress of the deprivation under color of statute, ordinance, regulation, custom or usage of certain rights secured to him by the Fourteenth Amendment to the United States Constitution and under the Illinois Constitution."

Bartlett claims that because of the curriculum requirement, he "displayed to his second-grade students several garden-variety tools, including a box cutter, a 2.25-inch pocketknife, wrenches, screwdrivers, and pliers. The visual aids were used in an effort to facilitate student understanding and remembrance of the curriculum. As he displayed the box cutter and pocketknife, plaintiff specifically described the proper uses of these tools. Neither of these items was made accessible to the students."

Nonetheless, the next day, "an area observer" complained about him. "As a result of this complaint, plaintiff was charged with possessing, carrying, storing, or using a weapon; negligently supervising children; inattention to duty; violating school rules; and repeated flagrant acts."

He was given a hearing in September, and Newell suspended him without pay for four days, according to the complaint.

He seeks nominal and compensatory damages for constitutional violations, and costs.

He is represented by Dmitry Feofanov with The Rutherford Institute, of Lyndon, Ill.



Just another victim of disastrous anti-White U.S. immigration policies.



Ask no questions! Do what you're told! They don't need warrants!

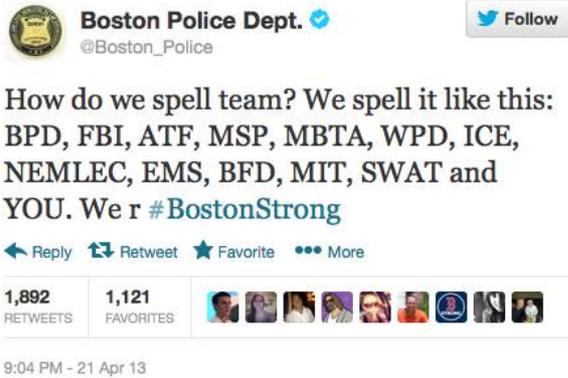


Ask no questions! They're there to protect you! You don't need a gun!

Remember: None of this militarized Hollywood-style circle jerk police action actually found the bomber!

He was found by a regular guy just checking on his boat. If anything, it created *more* confusion. This is also why you should be suspicious of organizations like the Oathkeepers. When push comes to shove, you can bet dirty cops will side with their cushy pension plans over the rights of the public.

I can GUARANTEE you nobody in the Watertown/Boston PD said "no" when asked to search a house or person without a warrant, or not to point their loaded weapons at the public (which is illegal, BTW)...



How do you spell "police state?"

BOSTON – National guard units seeking to confiscate a cache of recently banned assault weapons were ambushed on April 19th by elements of a para–military extremist faction. Military and law enforcement sources estimate that 72 were killed and more than 200 injured before government forces were compelled to withdraw.

Speaking after the clash Massachusetts Governor Thomas Gage declared that the extremist faction, which was made up of local citizens, has links to the radical right–wing tax protest movement. Gage blamed the extremists for recent incidents of vandalism directed against internal revenue offices. The governor, who described the group's organizers as "criminals," issued an executive order authorizing the summary arrest of any individual who has interfered with the government's efforts to secure law and order. The military raid on the extremist arsenal followed wide–spread refusal by the local citizenry to turn over recently outlawed assault weapons.

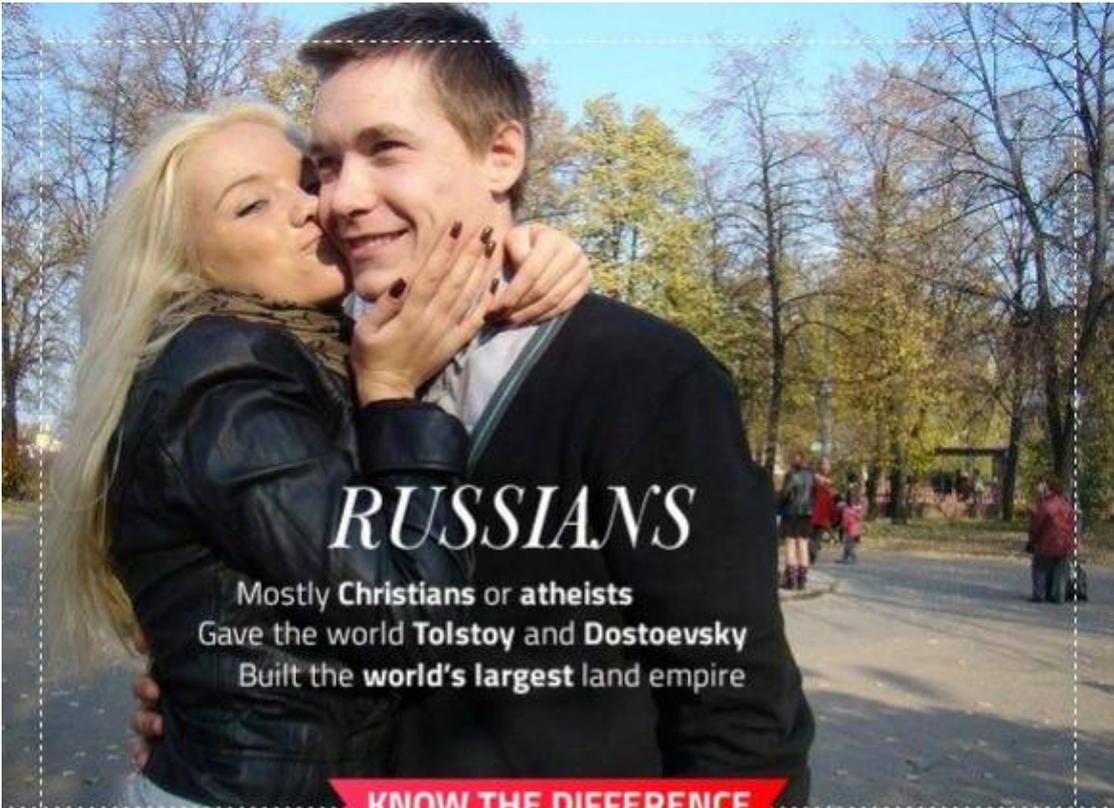
Gage issued a ban on military–style assault weapons and ammunition earlier in the week. This decision followed a meeting in early this month between government and military leaders at which the governor authorized the forcible confiscation of illegal arms.

One government official, speaking on condition of anonymity, pointed out that "none of these people would have been killed had the extremists obeyed the law and turned over their weapons voluntarily."

Government troops initially succeeded in confiscating a large supply of outlawed weapons and ammunition. However, troops attempting to seize arms and ammunition in Lexington met with resistance from heavily–armed extremists who had been tipped off regarding the government's plans. During a tense standoff in Lexington's town park, National Guard Colonel Francis Smith, commander of the government operation, ordered the armed group to surrender and return to their homes. The impasse was broken by a single shot, which was reportedly fired by one of the right–wing extremists. Eight civilians were killed in the ensuing exchange. Ironically, the local citizenry blamed government forces rather than the extremists for the civilian deaths. Before order could be restored, armed citizens from surrounding areas had descended upon the guard units.

Colonel Smith, finding his forces overmatched by the armed mob, ordered a retreat. Governor Gage has called upon citizens to support the state/national joint task force in its effort to restore law and order. The governor also demanded the surrender of those responsible for planning and leading the attack against the government troops. Samuel Adams, Paul Revere, and John Hancock, who have been identified as "ringleaders" of the extremist faction, remain at large.

--- April 20, 1775



RUSSIANS

Mostly **Christians** or **atheists**
Gave the world **Tolstoy** and **Dostoevsky**
Built the **world's largest** land empire

KNOW THE DIFFERENCE



CHECHENS

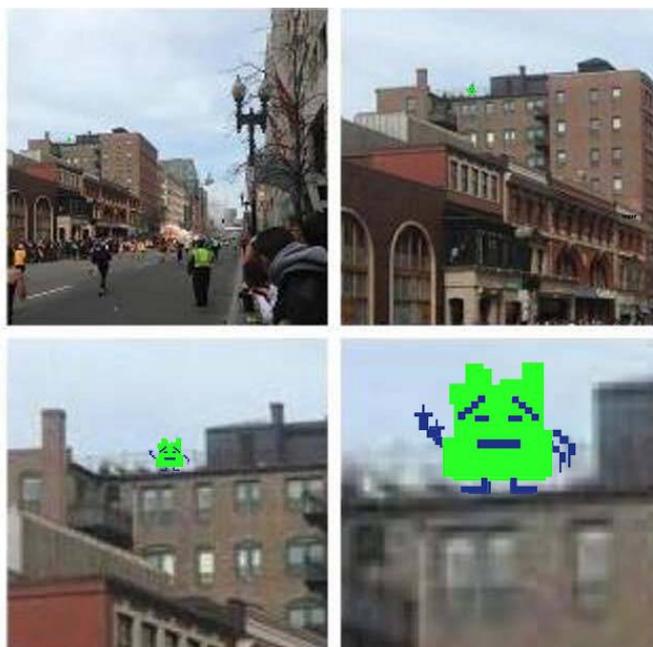
Mostly **Muslims**
Gave the world **Basaev** and **Tsarnaev**
Were granted a **tiny republic**
of their own by the **Soviets**

SPUTNIKIPOGROM.COM



Russians = Essentially hard-working, law-abiding, honest Whites. Russians are descendants of the Ruses, who were basically vikings from Sweden.

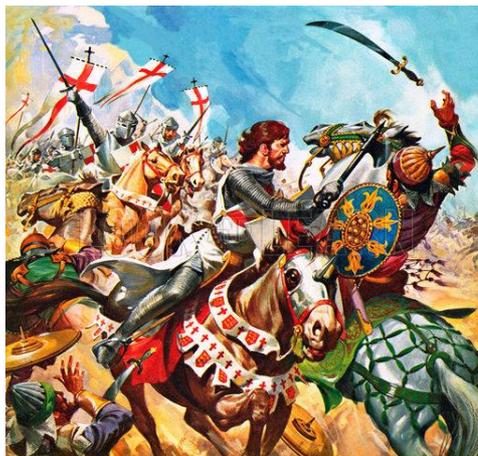
Chechens = Mongoloid Turks from Central Asia and the Caucasus region. Today's Caucasians are not Whites!





"I think there's a resurgence of anti-Semitism because at this point in time Europe has not yet learned how to be multicultural, and I think we're [anti-White Jews] gonna be part of the throes of that transformation, which must take place. Europe has not yet learned how to be multicultural. Europe is not going to be the monolithic societies that they once were in the last century. Jews are going to be at the center of that. It's a huge transformation for Europe to make. They are now going into a multicultural mode, and Jews will be resented because of our leading role. But without that leading role, and without that transformation, Europe will not survive."

--- Quote from [Barbara Lerner Spectre](#) interview with the Israeli Broadcasting Authority News, 2010. Search YouTube for the entire video of her interview. I'm pretty sure Europe could "survive" without Jewish multiculturalism and diversity!



"Tell MAMA" (tellmamauk.org) is a website which documents and outlines anti-Muslim "prejudice and hate" in the United Kingdom.

Be sure submit a few reports...

Report Title *

Scary Amrican threatn me

Description *

I am muslim n on the intrenets amrican said this to me

What the fuck did you just fucking say about me, you little bitch? I'll have you know I graduated top of my class in the Navy Seals, and I've been involved in numerous secret raids on Al-Quaeda, and I have over 300 confirmed kills. I am trained in gorilla warfare and I'm the top sniper in the entire US armed forces. You are nothing to me but just another target. I will wipe you the fuck out with precision the likes of which has never been seen before on this Earth, mark my fucking words. You think you can get away with saying that shit to me over the Internet? Think again, fucker. As we speak I am contacting my secret network of spies across the USA and your IP is being traced right now so you better prepare for the storm, maggot. The storm that wipes out the pathetic little thing you call your life. You're fucking dead, kid. I can be anywhere, anytime, and I can kill you in over seven hundred ways, and that's just with my bare hands. Not only am I extensively trained in unarmed combat, but I have access to the entire arsenal of the United States Marine Corps and I will use it to its full extent to wipe your miserable ass off the face of the continent, you little shit. If only you could have known what unholy retribution your little "clever" comment was about to bring down upon you, maybe you would have held your fucking tongue. But you couldn't, you didn't, and now you're paying the price, you goddamn idiot. I will shit fury all over you and you will drown in it. You're fucking dead, kiddo.

Date & Time: Today at 9:57 pm

[+ Modify Date](#)

Categories *

- Extreme Violence
- Assault
- Damage and Desecration of Properties
- Threats
- Abusive Behaviour
- Anti-Muslim Literature

Submit A Report

Report Title *

police brutally shoot two innocent muslims in the UK

Description *

two black Muslims with gardening tools were brutally attacked by British police with automatic weapons; their apparent crime was killing the infidel. You and I both know that this is hardly a crime and is frequently recommended by the qiran. these christian devils need to be taught a lesson and brought to justice under sharia law

Gender of Perpetrator

Male Female Unknown

Ethnicity of Perpetrator

White British

In your opinion, did the perpetrators have any Far Right Links to Extreme Groups?

Yes No Unknown

If Yes, can you provide further details?

they were evil white christians from the muslim hating british government

Have you reported this incident to the Police?

Yes No

If Yes, can you provide details of the (Police) officer working on your case?

they told me that Muslims were the scum of the earth and that all these religion based attacks are why the world is sick of your shit and is going to exterminate militant Islam from the face of the earth with fire and sword, just like last time. they then told me that us shitty bronze age dirt farmers cannot win and will either be left to exterminate each other in inter tribal feuding like barbarians or be put down like animals en masse and be buried in mass graves filled with pigs blood