Pulling the Curtain on Airport Security

Billy Rios
Xssniper@gmail.com
@xssniper

How to get put on the no-fly list…

Why are you doing this?

- Just an average Joe

- Interest in ICS, Embedded and Medical devices

- I travel a lot

Lessons Learned by a Young Butterbar

- Show respect

- Accept Responsibility

- Trust, but Verify

Show me the Money… (budget.house.gov)

- \> 50,000 people at more than 400 airports across the country and an annual budget of $7.39 billion (2014)

- TSA receives about $2 billion a year in offsetting collections under current law, through air-carrier and aviation-passenger security fees. The largest of the fees, in terms of total collections, is the Aviation Passenger Security Fee (sometimes called the September 11th Security Fee), which brings in about $1.7 billion a year.

- By law, the first $250 million of passenger-security fees is set aside for the Aviation Security Capital Fund, which provides for airport-facility modifications and certain security equipment

Show me the Money...

One guy

no budget

and a laptop

Disclosure

All issues in this presentation were reported to DHS

via ICS-CERT >6 months ago

Response?

- Our software "cannot be hacked or fooled"
- "add their own software and protections."
- <silence>
- Spoke with Morpho last week

Scenarios

(1) TSA doesn't know about the security issues in their software

(2) TSA knew about the security issues, developed their own custom fixes, never told the vendors… and is hording embedded zero day vulnerabilities and leaving other organizations exposed?

Recommended Security Guidelines for Airport Planning, Design and Construction

Transportation Security Administration

Revised: May 2011
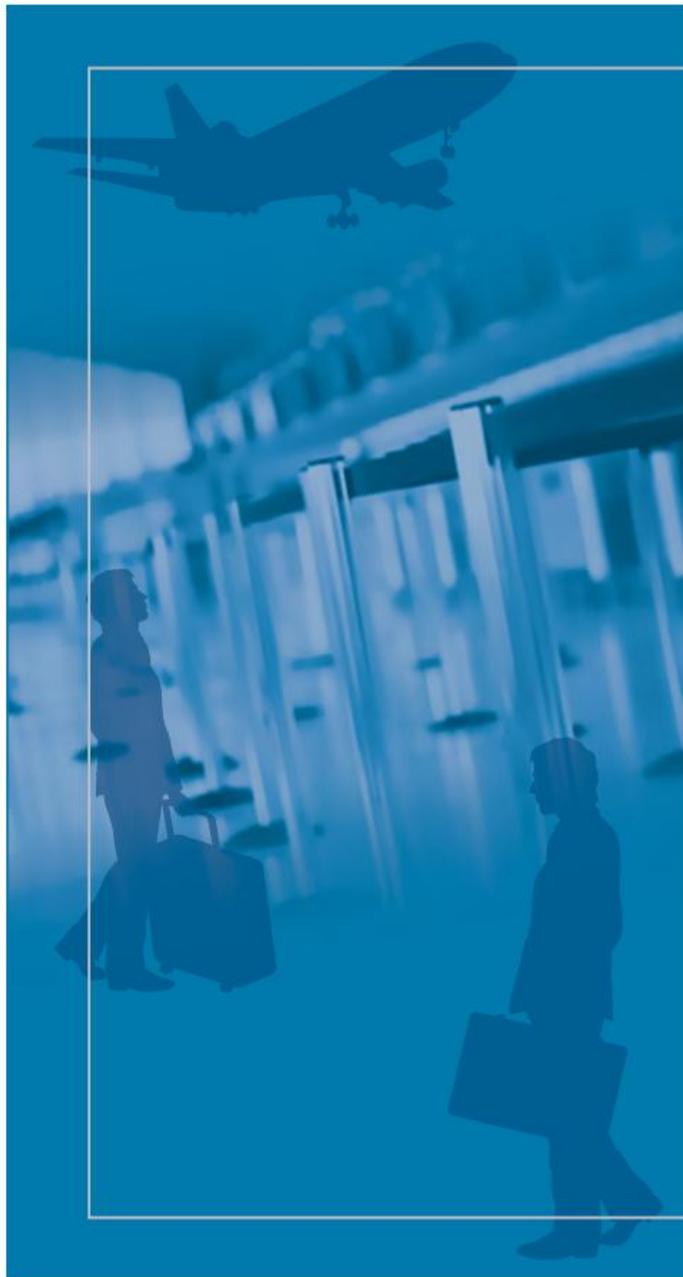
Transportation Security Administration

CHECKPOINT DESIGN GUIDE (CDG)
Revision 4.0
August 29, 2012

Prepared for the
Transportation Security Administration (TSA)

Office of Security Capabilities (OSC)
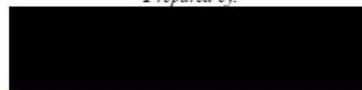
**Figure 1-2** Example SSCP

Isometric View
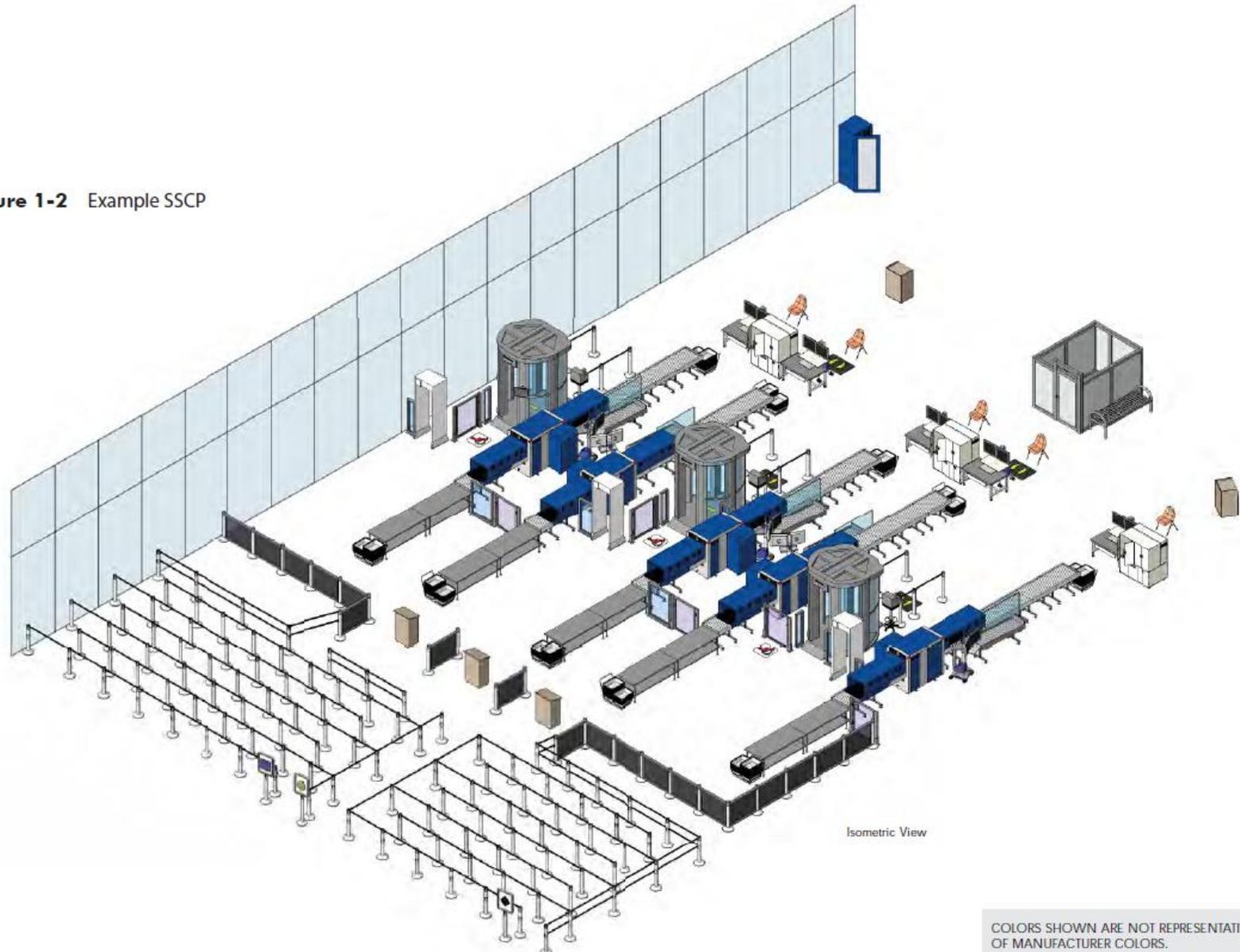
COLORS SHOWN ARE NOT REPRESENTATIVE
OF MANUFACTURER COLORS.

Figure 2-8 TDC Podium & CAT/BPSS

Equipment	Quantity	Power Requirements	IT Requirements	Additional Information
TDC Podium CAT/BPSS (generic)	1 per 2 lanes +1 for odd numbered lanes +1 if checkpoint feeds international flights	• Non-dedicated • 20A, 125V, 180VA/podium • 2-Pole, 3-Wire Grounding • NEMA 5-20R Duplex Receptacle • Power cord length is unknown at the time of this printing	• Data Drops = 2 • Cat5e / Cat6 cable • The cable length from the termination point in the IT cabinet to the data outlet in the work area shall not exceed 295'. • If data drop cannot be secured when the checkpoint is closed, a locking device is required. Coordinate with TSA HQ IT Security.	• The TDC function can be supported by either a TDC Podium or a CAT/BPSS. • The CAT/BPSS may be on wheels or it may sit on floor.

SIDE VIEW: PODIUM   ELEVATION   PLAN VIEW: PODIUM OR CAT/BPSS   SIDE VIEW: CAT/BPSS (GENERIC)   ELEVATION
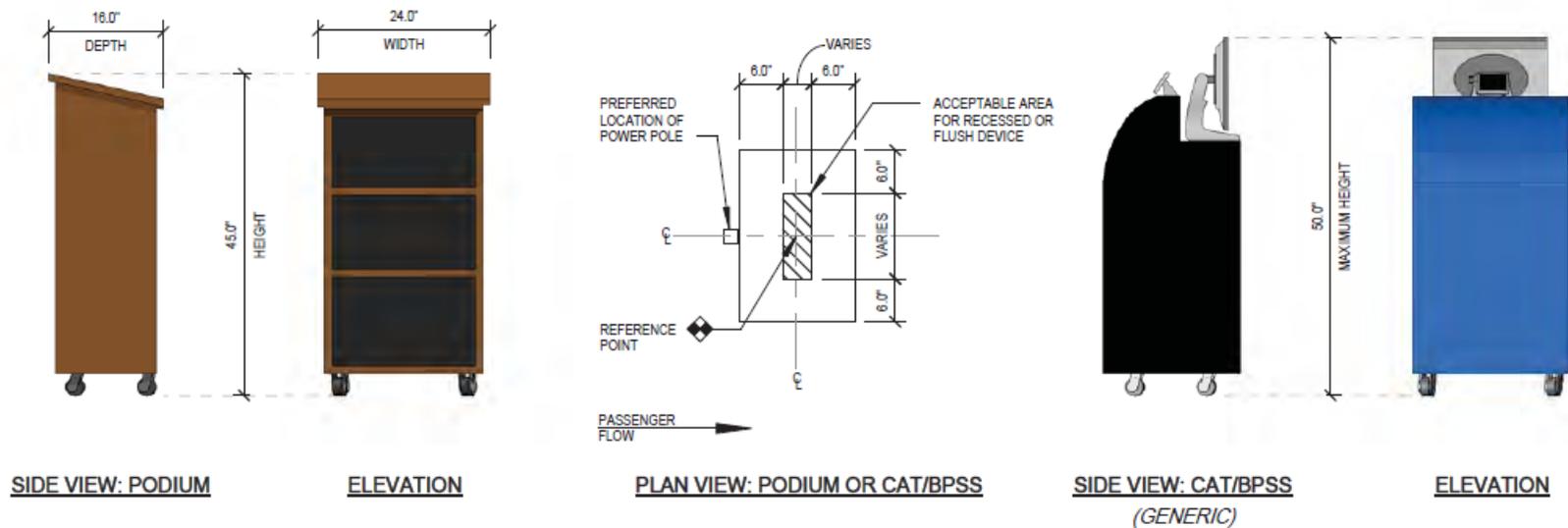
2.3 BIN CART

Bins are the gray containers located on a cart at the front and back of each checkpoint lane. Passengers use bins to divest themselves of their personal belongings such as purses, carry-on bags, backpacks, laptops, shoes, jackets, etc. Bin carts are similar to a hand cart or dolly that allows for the transport of a large number of bins without requiring excessive lifting or carrying by a TSA agent. In the past, bin transport by the TSOs was the primary cause of on-the-job injuries at checkpoints. Hand-carrying of bins is no longer endorsed by TSA. TSA recommends that bin carts be pushed upstream though an ADA or access gate. Ideally, an ADA or access gate should exist at every lane but this is not always possible. When there is insufficient space for an ADA or access gate, the bin cart should be pushed upstream against passenger flow through the WTMD.

Bin carts can be one or two bins wide with bins stacked on top to slightly below the handle which equates to approximately 40 bins. Each lane requires a bin cart at each end. TSA recommends maintaining about 60 bins per lane divided across each end. A fully-loaded bin cart should be located at the start of the divest tables on the non-sterile side of the lane for passenger pick-up. The other bin cart should be positioned at the end of the composure rollers on the sterile side so that the TSA agent can collect empty bins after passengers have picked up their belongings. Refer to **Figure 2-9** for bin cart dimensions. The bin cart width times two should be factored into the overall length of the checkpoint lane when designing a new checkpoint or reconfiguring an existing checkpoint.

Figure 2-9 Bin Cart

20.5" WIDTH

PLAN VIEW

32.5"
LENGTH

APPROX. 30 BINS

ELEVATION
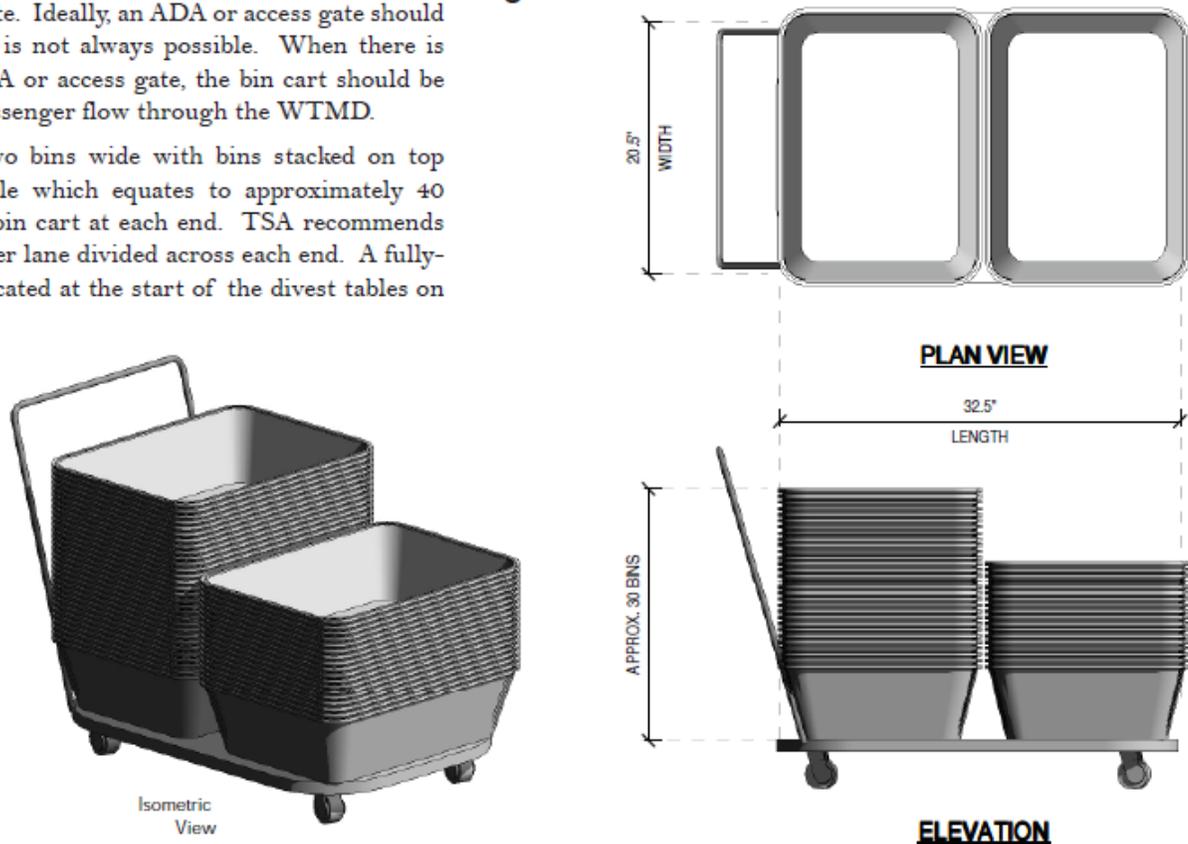
Isometric View

ETD
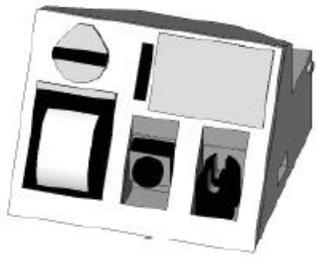
GE IonTrack Itemiser
Isometric View

GE IonTrack Itemiser³
Isometric View

Smiths IonScan 400B
Isometric View

Smiths IonScan 500DT
Isometric View

BLS

CEIA EMA-MS
Isometric View
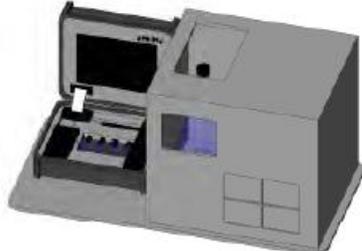
Smiths RespondeR RCI
Isometric View

KRONOS TERMINAL MOUNTED
OVER LAN PORT AND SECURED
FLUSH ON WALL WITH NO
EXPOSED CABLING

54" MAX

9" MIN

IT Requirements	Additional Information
• Data Drops = 2 • Cat5e / Cat6 cable • The cable length from the termination point in the IT cabinet to the data outlet in the work area shall not exceed 295'. • If data drop cannot be secured when the checkpoint is closed, a locking device is required. Coordinate with TSA HQ IT Security.	• The TDC function can be supported by either a TDC Podium or a CAT/BPSS. • The CAT/BPSS may be on wheels or it may sit on floor.

Figure 4-1   SSCP Data Connectivity Diagram
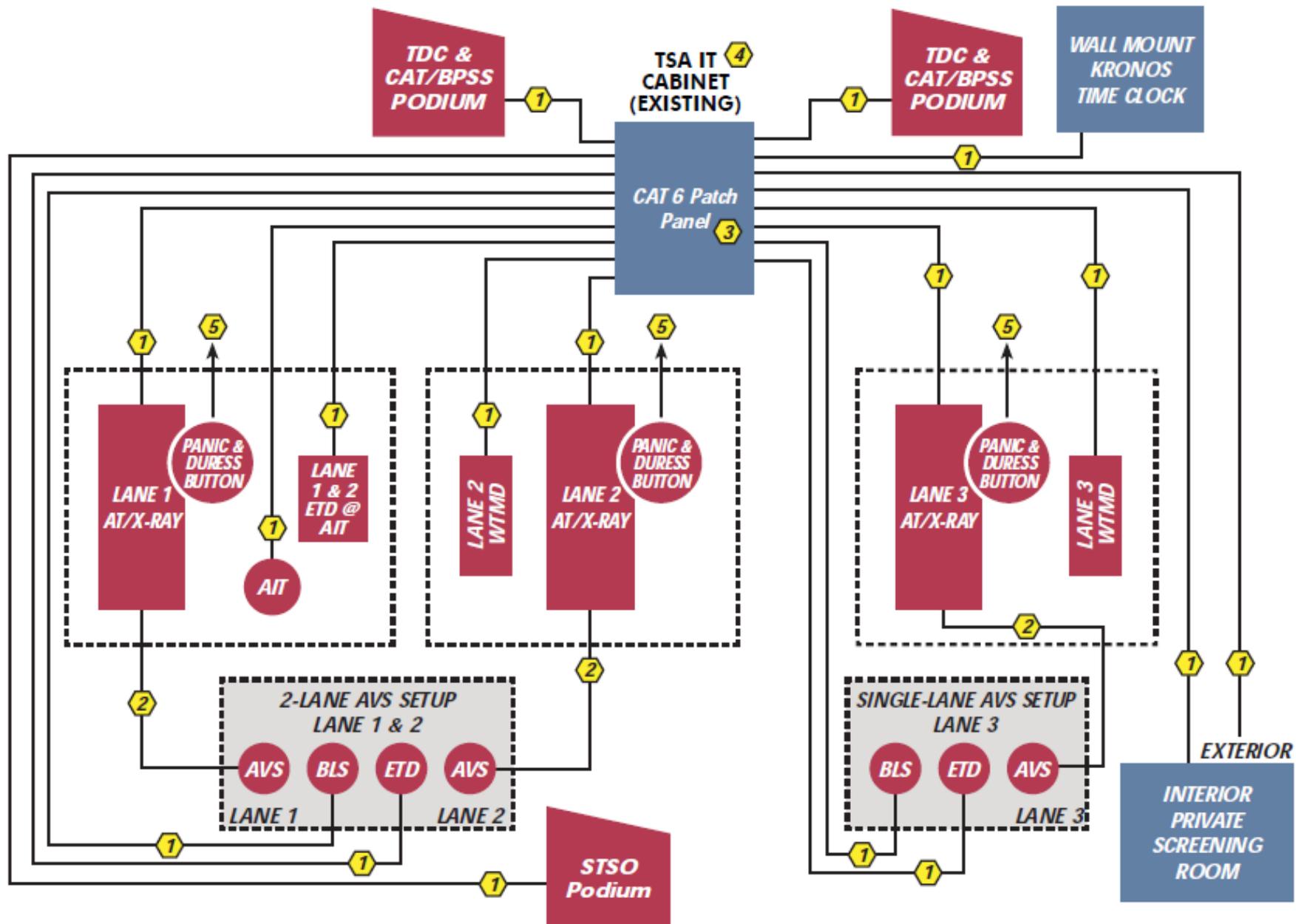
IT Program Assessment

TSA- Security Technology Integrated Program (STIP) (2010)

Review

The DHS Chief Information Officer conducted a comprehensive program review of the TSA - Security Technology Integrated Program (STIP) on April 15, 2010. The STIP program, a joint effort co-funded by the Passenger Screening Program (PSP) and Electronic Baggage Screening Program (EBSP), is a TSA-wide Enterprise system that delivers data from passenger and baggage screening security technologies (in a common format) in order to facilitate data interchange/exchange through a single network for effective communication and metrics reporting. STIP has Enterprise Management, Configuration Management, Resource Management and Equipment Maintenance capabilities.

TSANET   Category X Airports

A Quick Lesson on Backdoors

I can't believe it, Jim. That girl's standing over there listening and you're telling him about our back doors?

Yeah, but your giving away our best tricks!

[*Yelling*] Mr. Potato Head! Mr. Potato head! Backdoors are not secrets!

They're not tricks!

A Word About Backdoors

- Malicious account added by a third party

- Debugging accounts that someone forget to remove

- Accounts used by Technicians for Service and Maintenance

Technician Accounts == Backdoors

- Often hardcoded into the software

- Applications which depend on the passwords

- Business process which depend on passwords

- External software which depend on passwords

- Training which train technicians to use these passwords

Technician Accounts == Backdoors

- Can be discovered by external third parties (like me!)

- Cannot be changed by the end user (in most cases)

- Once initial work is completed, these passwords usually scale

Rapiscan 522B

—RAPISCAN THREAT IMAGE PROJECTION—

HIT

MISS
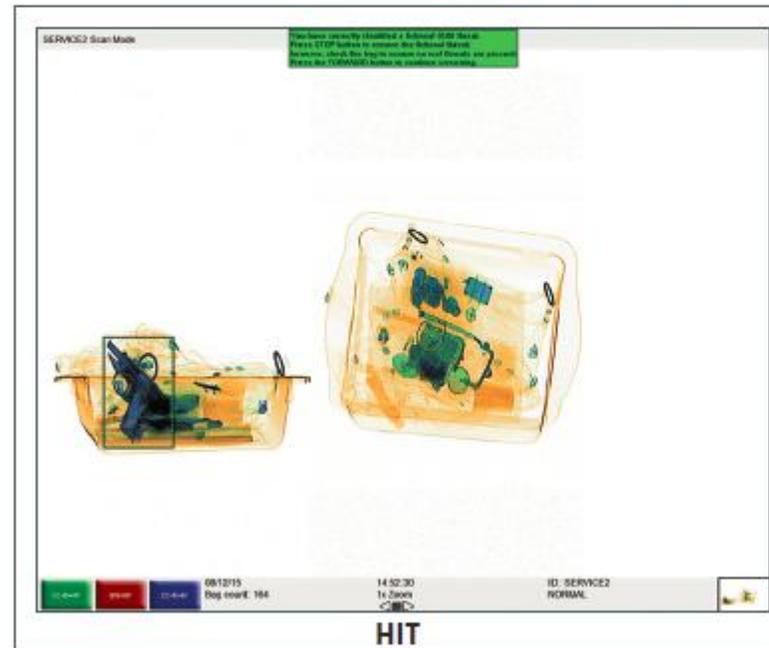
Microsoft®

Windows®xp

Professional

Copyright © 1985-2001
Microsoft Corporation
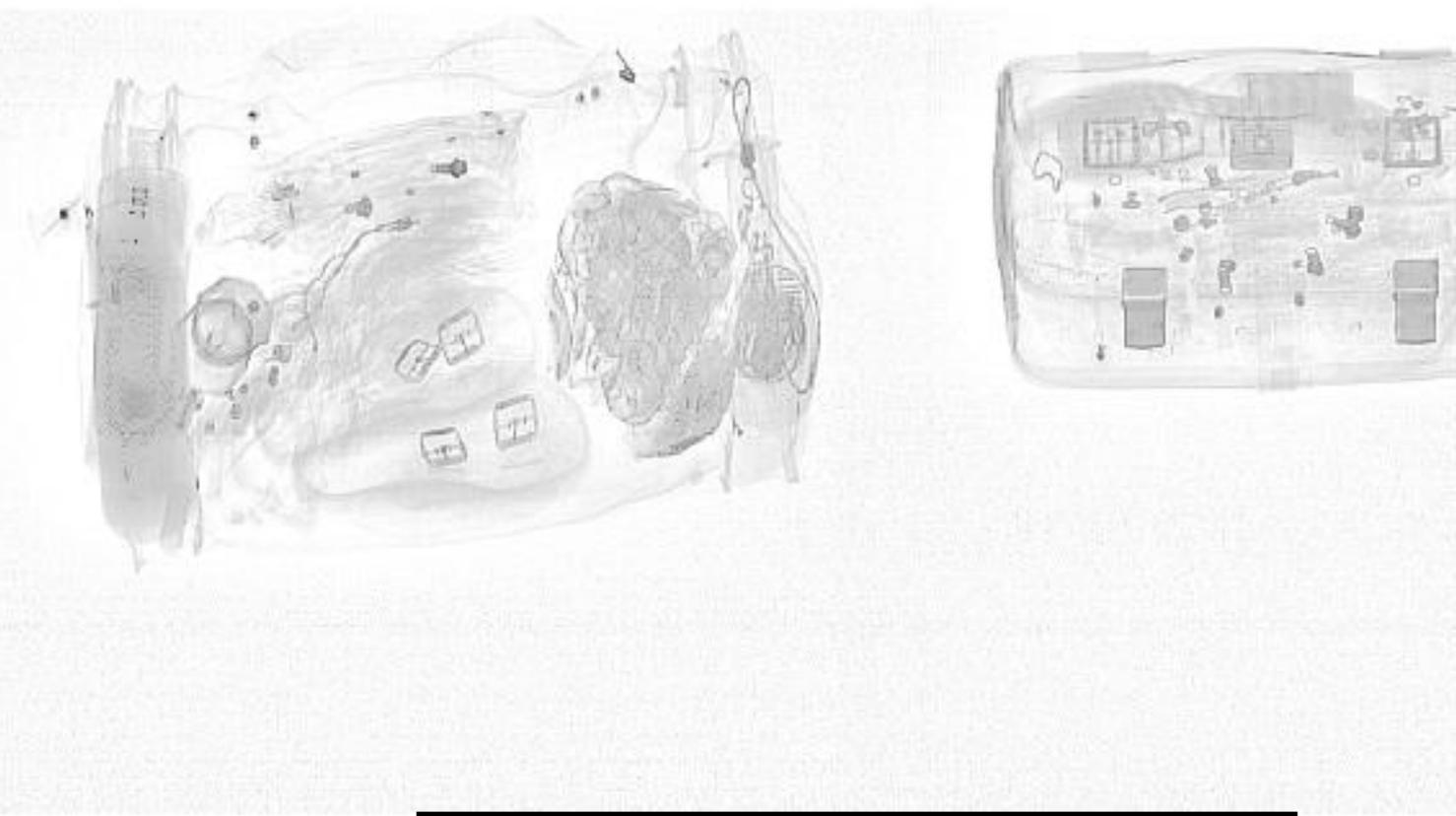
```
USERS.CFG

200        NUMBER_ERG_BIT                12          ; After classify energy
201        ENERGY_TYPE_FLAG              0           ; 0 == DUAL ENERGY, 1 == HIGH, 2 == LOW
202        CLASS_TBL_CLASS_DIV         349   349    349            ; 1st interval 349-240, 2nd
203        CLASS_TBL_ENERGY_DIV         20   300    301    900   ; 1st interval 0-100; 100-30
204
205
206    [MAP_CONTROL]
207        FULL_MAP_FILE                     C:\rapiscan\lut\r522bp_f.map
208        SKIP_MAP_FILE                     C:\rapiscan\lut\r522bp_s.map
209
210
211    [SYS_INFO]
212        OPID_OPTION          0     ; 0 = disable
213        FOOTMAT_OPTION       0     ; 0 = disable
214        RAP_PASSWORD              2830
215        CURTAIN_SW_DELAY          40
216        FOOTMAT_OPEN_DELAY        50
217        MONOCHROME_FLAG           0           ; 0 = color, 1 = monochrome
218        EXTRA_SCAN_CTRL           0           ; 0 = disable (for Auto Bringback)
219        BIDIR_SCAN_FLAG      0     ; 0=FWD,1=REV,2=BIDIR,3=FW+AB,4=REV+AB
220        SAFETY_TRIP_OPTION   0     ; 0 = disable
```

TIP - [Log On]

Log On

ID | 0011

Password | *****

[OK]   [Cancel]

USER

	User_ID	First_Name	Middle_Ini	Last_Name	CharCntInPa	Password	AccessCode	ActiveCode
⊞	0011	Service		Engineer	0	0011	1	1
⊞	1234	Temporary		SCREENER	0	1234	7	1
*					0		0	0

C:\Users\BK\Desktop\Rapiscan\working\SPEARS\DBASE\USER_RCR.CFG - Notepad++

File   Edit   Search   View   Encoding   Language   Settings   Macro   Run   Plugins   Window   ?

USER_RCR.CFG

```
1   NULNULNULNULNULServiceNUL      NUL      EngineerNUL       NUL0011NUL          0011NUL
```

Main   Report   TIP Utilities   Help

Log On

ID   z'or+1=1—

Password   *|

OK   Cancel

TIP - [Log On]

Main   Report   TIP Utilities   Help

Log On

TIP

Data Integrity problem in User's record

OK

P

OK   Cancel

Start   TIP - [Log On]   10:56 PM

Main   Report   TIP Utilities   Help

RAPISCAN Security Products

TIP

```
try {
        if (Checkpassword()){
                Authenticate();
        }
        Else{
                AuthFail();
        }
}
catch{
        ShowErrorMessage();
        Authenticate();
}
```

RAPISCAN THREAT IMAGE PROJECTION

HIT

MISS
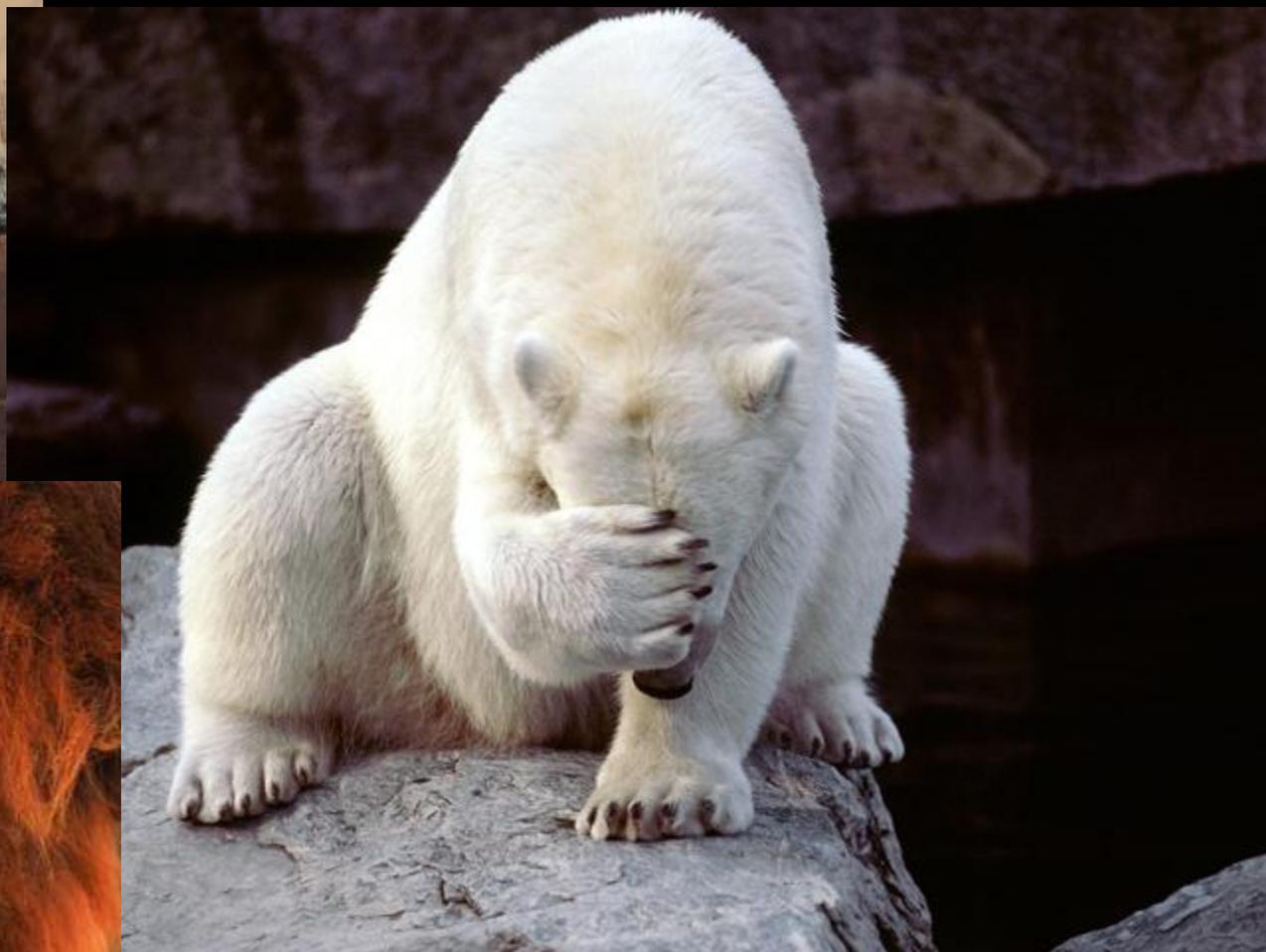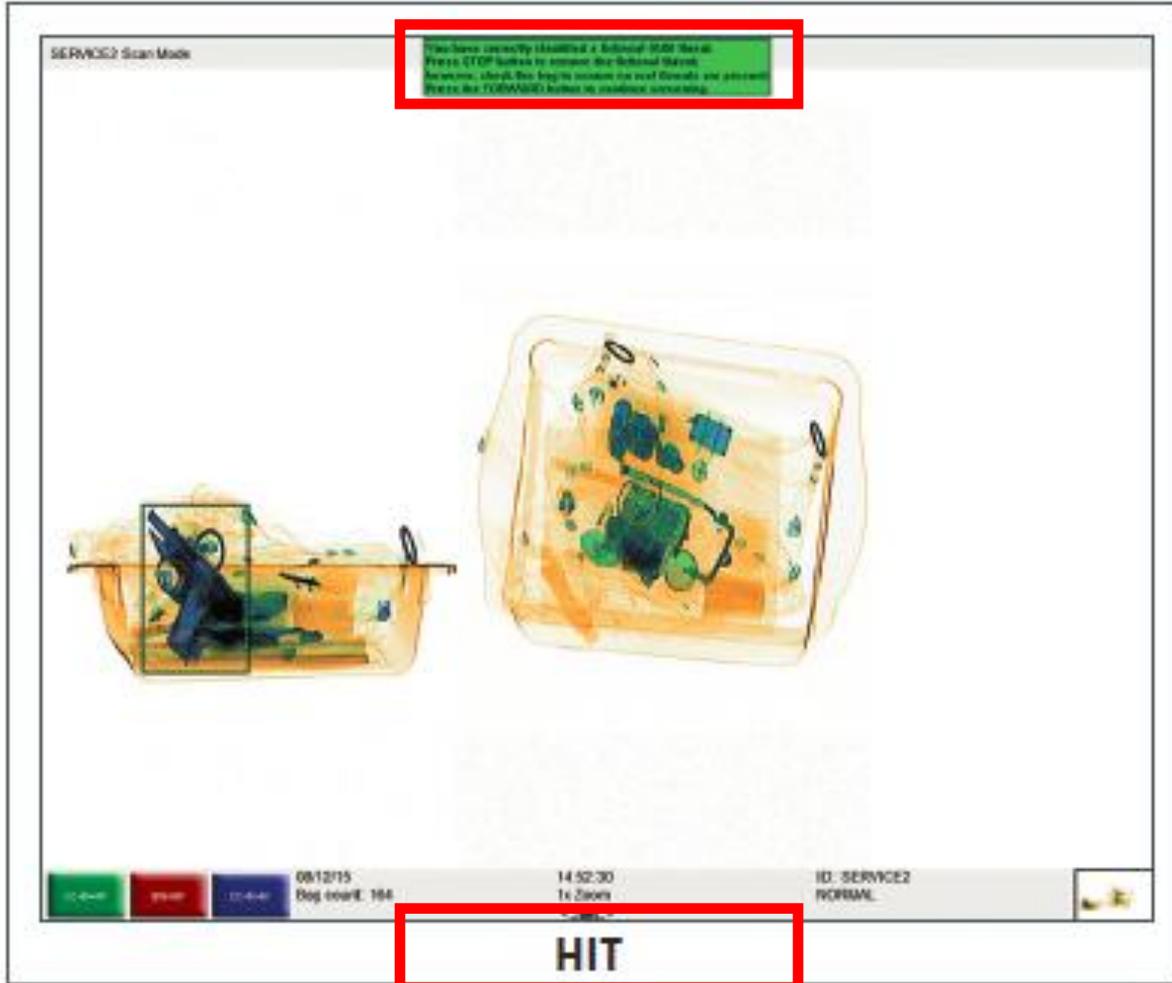
Name ▲

📁 BOMB
📁 CTI
📁 GUN
📁 HAZARD
📁 KNIFE
📁 OTHER

🖼 8MM1AKCG.BMP
📄 8MM1AKCG.FTI
🖼 8MM1BKCG.BMP
📄 8MM1BKCG.FTI
🖼 8MM1CKCG.BMP
📄 8MM1CKCG.FTI
🖼 8MM2AKCG.BMP
📄 8MM2AKCG.FTI
🖼 8MM2BKCG.BMP
📄 8MM2BKCG.FTI
🖼 8MM2CKCG.BMP
📄 8MM2CKCG.FTI
🖼 GUN1V1.BMP
📄 GUN1V1.FTI
🖼 GUN1V2.BMP
📄 GUN1V2.FTI
🖼 GUN2V1.BMP
📄 GUN2V1.FTI
🖼 GUN2V2.BMP

E:\Rapiscan\TIM\GUN\CONV\8MM1AKCG.FTI - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

8MM1AKCG.FTI

```
1   8MM1AKCG[NUL]arian keychain gun, .32 caliber[NUL][NUL][NUL][NUL][NUL][NUL][N
2   [SI]Ó[SI]|[SI]Æ[SI]Ó[SI]¢[SI]‹[SI]À[SI]¦[SI]Å[SI]¥[SI]‹[SI]ø[SI]Ô[SI]å[SI]Û[SI]ÿ[SI]»[SI]ª[SI]Ì
3   [SO]'[SO]
4   [SO]–[SO]J[SO][DLE][SO][DC3][SO][FF][SO]¹
5   ÿ
6   #[SO],[SO]‹[SO]ï
7   Y[SO][VT][SO]°
8   å
9   ß
10  Ä
11  á
12  ©
13  ö
14  ‡
15  @[SO]~
16  ,[SO]½
17  H[SO]Ü
18  A[SO]2[SO]©[SO][SO][SI][SI][DC2][SI]t[SI]E[SI]ÿ[SI]„[SI]Ó[SI]À[SI]‡[SI]Í[SI]ž[SI]Û[SI]{[SI]á[SI]ı
19  à[SO][SUB][FF]¶
```
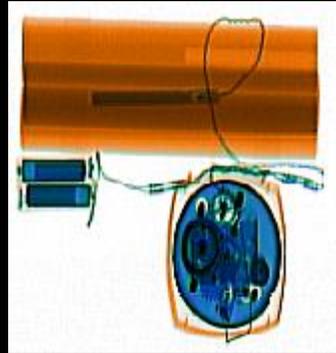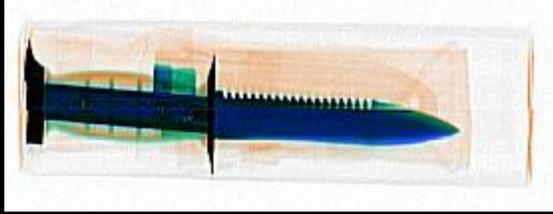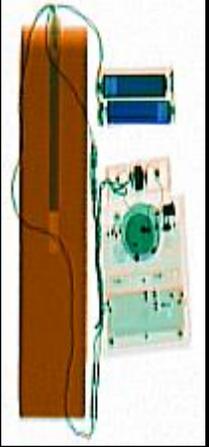
"TSA has strict requirements that all vendors must meet for security effectiveness and efficiency and does not tolerate any violation of contract obligations. TSA is responsible for the safety and security of the nearly two million travelers screened each day."

http://www.bloomberg.com/news/2013-12-06/naked-scanner-maker-osi-systems-falls-on-losing-tsa-order.html

"Questions remain about how the situation will be rectified and the potential for unmitigated threats posed by the failure to remove the machinery," the committee's Republican and Democratic leaders wrote in a Dec. 6 letter to the men. "It is our understanding that these new components -- inappropriately labeled with the same part number as the originally approved component -- were entirely manufactured and assembled in the People's Republic of China."

http://www.nextgov.com/defense/2013/12/congress-grills-tsa-chinese-made-luggage-scanner-parts/75098/

"The referenced component is the X-ray generator, a simple electrical item with no moving parts or software."

He described the piece as "effectively, an X-ray light bulb."
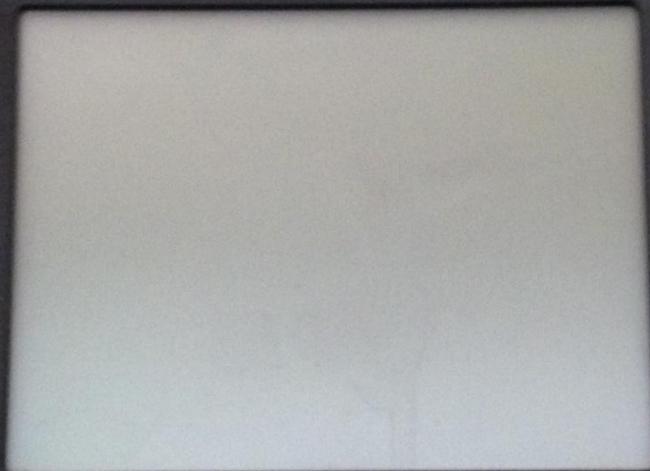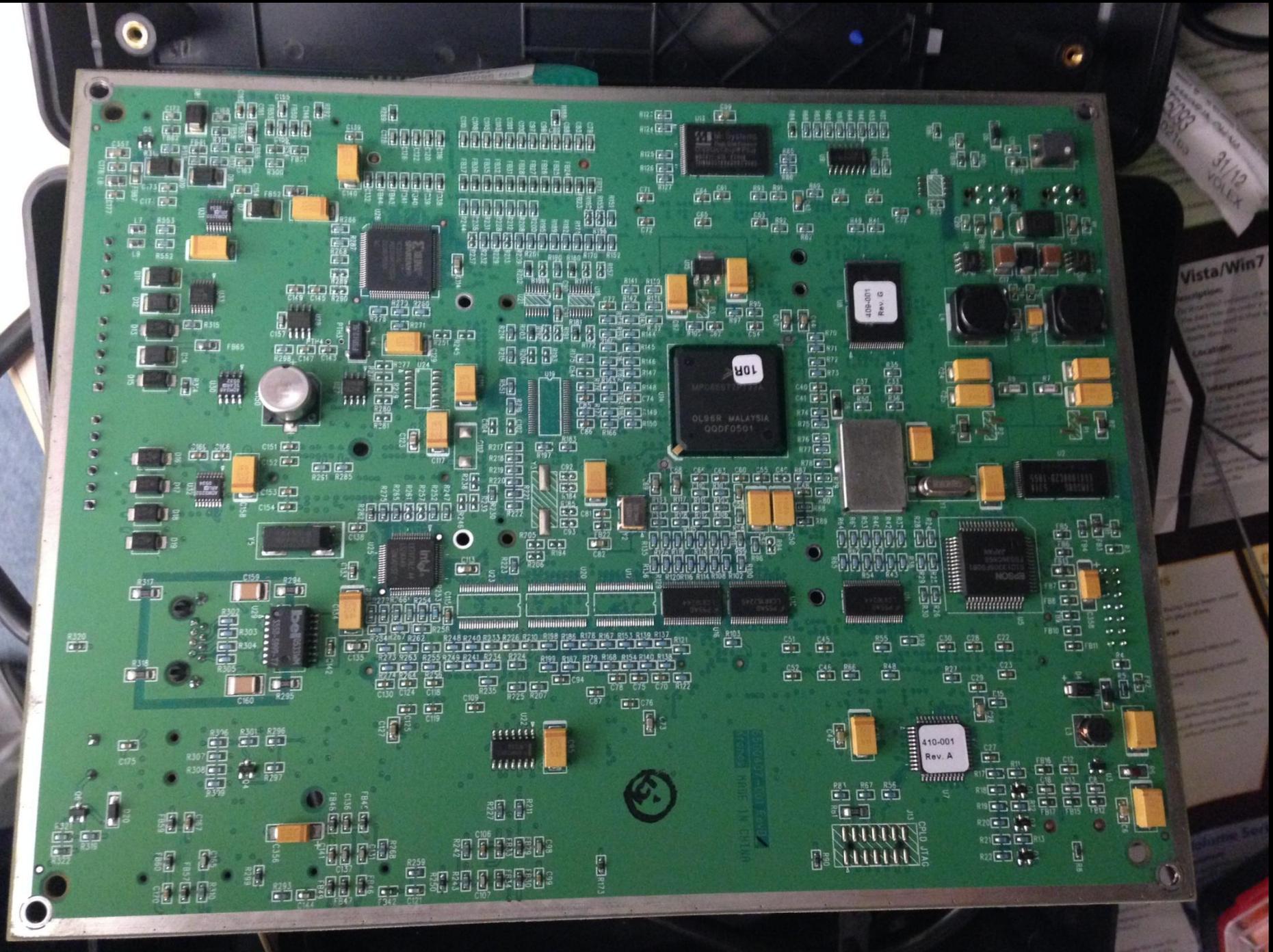
R90

C52

6500407-001 RevD

Kronos MADE IN CHINA

R122

R156

C73

Interesting Items

- VxWorks on PowerPC

- VxWorks FTP

- VxWorks Telnet

- Web server
  - Server: Allegro-Software-RomPager/4.32
  - WWW-Authenticate: Basic realm="Browser"

```
192.168.0.102 - PuTTY

value = 127 = 0x7f
-> devs
drv name
  0 /null
  1 /tyCo/0
  1 /tyCo/1
  2 /aioPipe
  5 /bpf/dhcpc
  5 /bpf/dhcpc-arp
  6 /pty/telnet.S
  7 /pty/telnet.M
  8 /beeper
  9 /MLkeypad/local
 10 /IOSIMkeypad/
  3 /flash0/
 11 /reader/bc/local
 12 /reader/bc/remote1
 13 /reader/bc/remote2
 14 /reader/bc/wand
 15 /reader/mag/local
 16 /lcd
 17 /reader/prox/local
 18 /reader/prox/remote
```

```
192.168.0.102 - PuTTY

value = 1 = 0x1
-> ifShow
fec (unit number 0):
     Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 192.168.0.102
     Broadcast address: 192.168.0.255
     Netmask 0xffffff00 Subnetmask 0xffffff00
     Ethernet address is 00:40:58:04:29:16
     Metric is 0
     Maximum Transfer Unit size is 1500
     0 octets received
     0 octets sent
     2210 packets received
     882 packets sent
     876 unicast packets received
     878 unicast packets sent
     1334 non-unicast packets received
     4 non-unicast packets sent
     0 input discards
     0 input unknown protocols
     0 input errors
     0 output errors
     0 collisions; 0 dropped
lo (unit number 0):
     Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
     Type: SOFTWARE_LOOPBACK
     Internet address: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
```

```
value = 0 = 0x0
-> cd "app"
value = 0 = 0x0
-> ls

.

..

M8M.jar
WebC.out
value = 0 = 0x0
->
```

```
value = 25 = 0x19
-> java
Usage: java [-options] class

where options include:
    -help               print out this message
    -version            print out the build version
    -v -verbose         turn on verbose mode
    -debug              enable remote JAVA debugging
    -noasyncgc          no effect.  Asynchronous GC support was removed.
    -verbosegc          print a message when garbage collection occurs
    -noclassgc          disable class garbage collection
    -ss<number>         set the maximum native stack size for any thread
    -oss<number>        set the maximum Java stack size for any thread
    -ms<number>         set the initial Java heap size
    -mx<number>         set the maximum Java heap size
    -mr<number>         set the red heap reserve size
    -my<number>         set the yellow heap reserve size
    -D<name>=<value>    set a system property
    -classpath <directories separated by colons>
                        list directories in which to look for application classes
    -bootclasspath <directories separated by colons>
                        list directories in which to look for system classes
    -Xrun<library>[:<option>=<value>,...]
                        load library on startup
    -verify             verify all classes when read in
    -verifyremote       verify classes read in over the network [default]
    -noverify           do not verify any class
value = 1 = 0x1
->
```

```
BootLine="tffs(0,0)Null:/flash0/os/vxWorksZ e=192.168.0.
hostname="Null"
ipAddr="192.168.0.102"
subnetMask="ffffff00"
gateway="192.168.0.1"
deviceId="444444"
bootBuildNbr="1000"
ftpUname="SuperUser"
ftpPassword="2323098716"
basicAuth="yes"
dhcp="no"
dhcpLeaseTime="-1"
hostServerIP="127.0.0.4"
keypad="telephone"
ModemId="02"
```

```java
}
String s6 = (String)hashtable.get("TelnetChoice");
if(s6 != null && s6.compareTo(DBTransaction.yesNo[0]) == 0)
{
    String s1 = M8MApp.devMgr.request("get|Configuration|nvParams^ftpUname#");
    if(s1.equals("?"))
    {
        String s2 = M8MApp.devMgr.request("set|Configuration|nvParams^ftpUname#SuperUser");
        s2 = M8MApp.devMgr.request("set|Configuration|nvParams^ftpPassword#2323098716");
        flag = true;
    }
} else
{
    String s3 = M8MApp.devMgr.request("get|Configuration|nvParams^ftpUname#");
```

Protected Object

216.9.106.24
San Francisco International Airport
Added on 26.05.2014

🇺🇸 Boulder Creek

Details

HTTP/1.0 401 Unauthorized

WWW-Authenticate: Basic realm="Browser"

Content-Type: text/html

Transfer-Encoding: chunked

Server: Allegro-Software-RomPager/4.32

Connection: close

Telnet

```
gt400-1 login:
```

HTTP

➡

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="Browser"
Content-Type: text/html
Transfer-Encoding: chunked
Server: Allegro-Software-RomPager/4.32
Connection: close
```

FTP

```
220 VxWorks (5.4.2) FTP server ready
530 Login failed.
214-The following commands are recognized:
HELP USER PASS QUIT LIST NLST
RETR STOR CWD TYPE PORT PWD
```

Backdoors…

- FTP and Telnet - SuperUser:2323098716
  - config\devCfg.xml file
  - MaintValidation.class file within the m8m.jar

- Web - KronosBrowser:KronosBrowser

- ~6000 on the Internet, two major airports

Here's a thought…

- Foreign made main board on TSA Net that can track which TSA personnel are on the floor at any given moment

- Hardcoded FTP password/backdoor

- Hardcoded Telnet password/backdoor which gives up a VxWorks shell

- Hardcoded Web password/backdoor

Does TSA know Kronos 4500's have Chinese made main boards?

Does the TSA know the software has hardcoded backdoors?

Trust but Verify the Engineering

Itemiser®

Dual Mode

No Alarm - Ready

Version 8.17
Super User 2

Log Off | Clear | Trigger | Help | Menu | Prev. View | Reset View

Plasmagram | Select Scan | Intensity Map | Processed 3D | Measure | Pan | Zoom

Neg Ion Peaks		Pos Ion Peaks	
Time	Height	Time	Height

Negative Ions: Cal:0.926 Offset:0.000 (Cal Units)

12000

10000

8000

6000

4000

2000

0

0   2   4   6   8   10   12   14

Positive Ions: Cal:0.926 Offset:0.000 (Cal Units)

12000

10000

8000

6000

4000

2000

0

0   2   4   6   8   10   12   14

Click here to begin

Switch Mode

Explosives Temperature & Library

Narcotics Temperature & Library

Dual Temperature & Library

Cancel
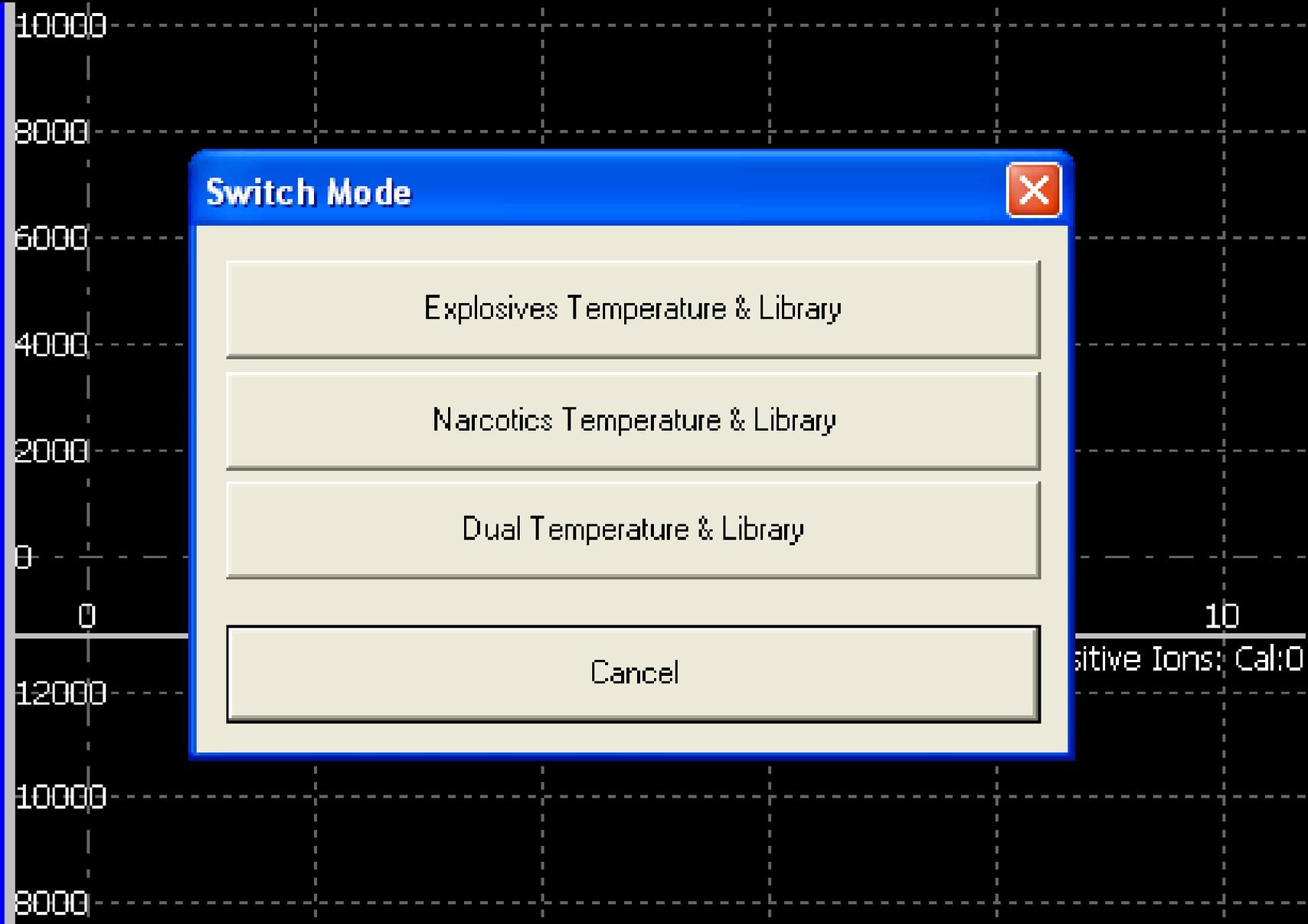
Pos Ion Pe
Time   He

Substance Selection

Name	Standard Location	Calibrated Location			Selected	Current Strength	Alarm Level
TNT	6.070	6.555	-0.040	+0.040	yes	0.00	750.0
NITRO	3.830	4.136	-0.100	+0.120	yes	0.00	750.0
RDX	6.350	6.857	-0.040	+0.040	yes	0.00	1000.0
PETN	7.990	8.629	-0.040	+0.040	yes	0.00	150.0
HMX	7.070	7.635	-0.040	+0.040	yes	0.00	1500.0
AM NO3	4.532	4.894	-0.040	+0.040	yes	0.00	1500.0
TATP	4.120	4.449	-0.040	+0.040	yes	0.00	750.0
TATP2	4.440	4.795	-0.040	+0.040	yes	0.00	750.0
SmklsPwdr	7.449	8.044	-0.040	+0.040	yes	0.00	250.0
COCAINE	7.936	8.570	-0.040	+0.040	yes	0.00	750.0
HEROIN	8.822	9.527	-0.040	+0.040	yes	0.00	500.0
THC	8.757	9.457	-0.040	+0.040	yes	0.00	500.0
METHAM	5.753	6.213	-0.040	+0.040	yes	0.00	500.0
AMPHET	5.664	6.117	-0.040	+0.040	yes	0.00	500.0
MDMA	6.375	6.884	-0.040	+0.040	no	0.00	500.0
MDA	6.275	6.776	-0.040	+0.040	no	0.00	500.0
MORPH	7.596	8.203	-0.040	+0.040	no	0.00	750.0
Ephedrine	5.953	6.429	-0.040	+0.040	yes	0.00	1000.0
Neg-CAL	6.070	6.555	-0.080	+0.080	no	0.00	1000.0
Pos-CAL	7.936	8.570	-0.080	+0.080	no	0.00	500.0

☑ Selected   Add   Modify   Delete   OK   Cancel

5 Offset

12
5 Offset

4000

Itemiser

- X86 (Pentium Processor)

- Windows CE

- Disk on chip with ~7.5 meg main program

- PS2, Floppy, USB

- IrDA?!?!?!?!

File System

- ITMSCE.exe (Main Application)

- Users.bin (User Accounts)

- Config.bin (Settings for detection)

- Options.bin

- History.bin

- Alarms (folder)

```
 ume in drive C is Ac
  lume Serial Number is 2525-15FB
 irectory of C:\

CONFIG     SYS             33 04-02-02    9:30a
SYS        COM         18,526 02-14-97    6:22a
AUTOEXEC   BAT             51 09-30-02    1:01p
NK         BIN      6,456,335 09-04-02    9:32a
LOADCEPC   EXE         95,868 07-11-02    4:44p
DOC-SST    BAT            269 09-30-02    2:43p
ITMSWIN        <DIR>          10-02-02    4:04p
COMMAND    COM         28,547 02-14-97    6:22a
HIMEM      SYS         29,136 09-30-93    4:20a
CAL        BIN             56 05-26-11   11:13a
 SERIAL    NUM             12 05-13-04   10:05a
        11 file(s)     6,628,833 bytes
                     119,793,664 bytes free

C:\>copy *.sys a:
Overwrite A:\CONFIG.SYS (Yes/No/All)?A
C:\HIMEM.SYS
        2 File(s) copied

C:\>
C:\>copy *.com a:_
```

Contains Radioactive Ma...
...mCi (370 MBq) Ni...
...rack Instruments
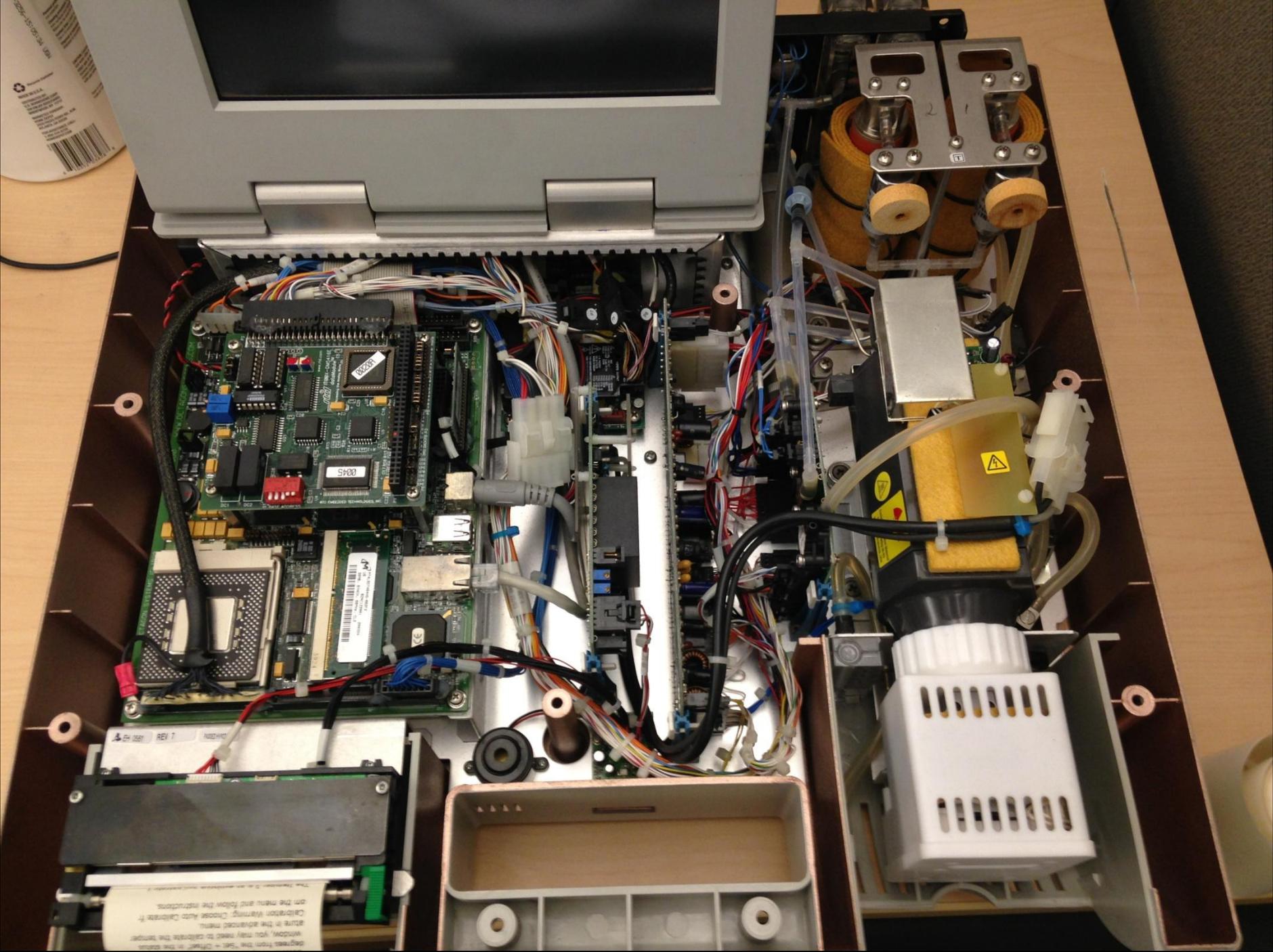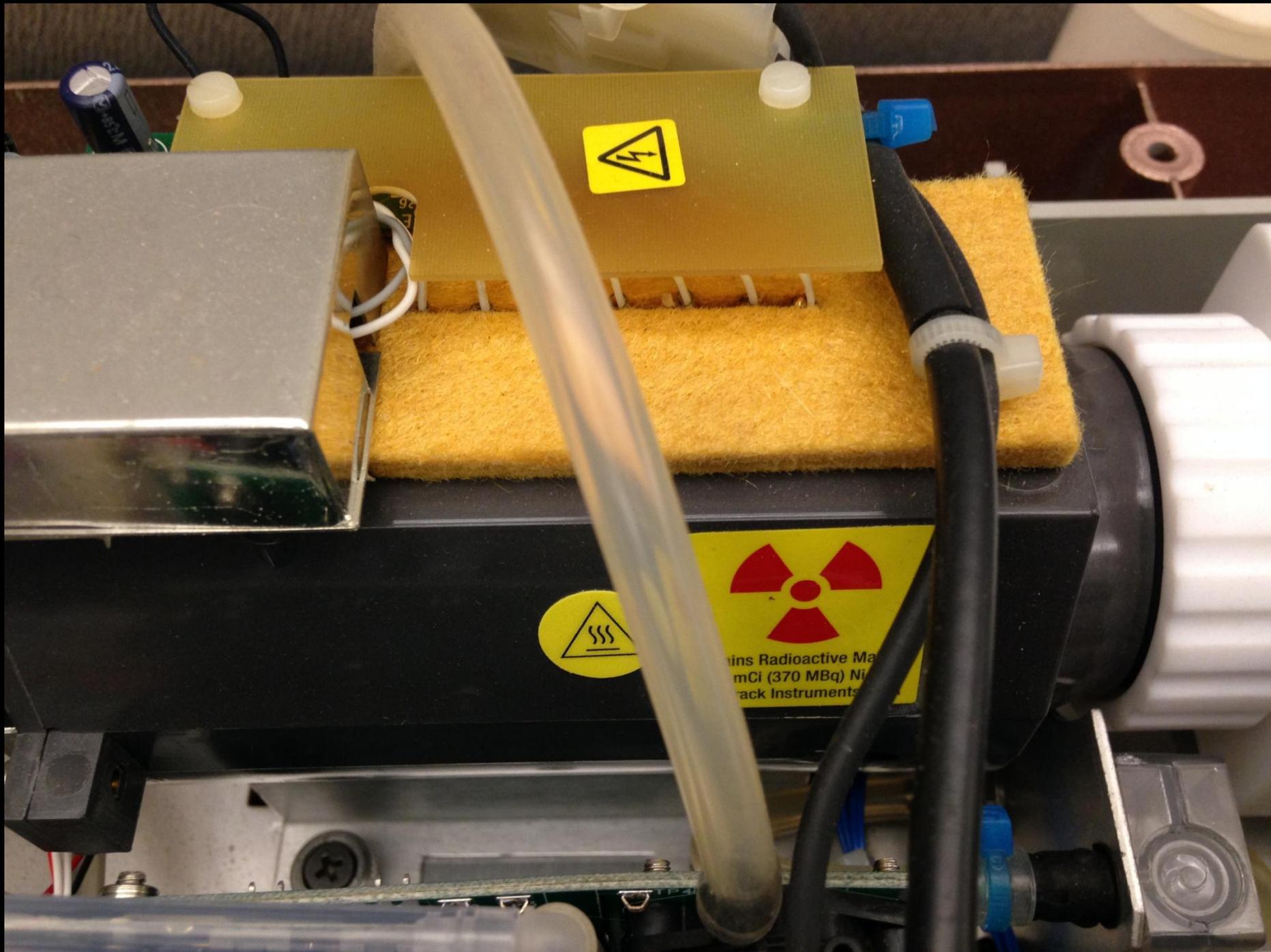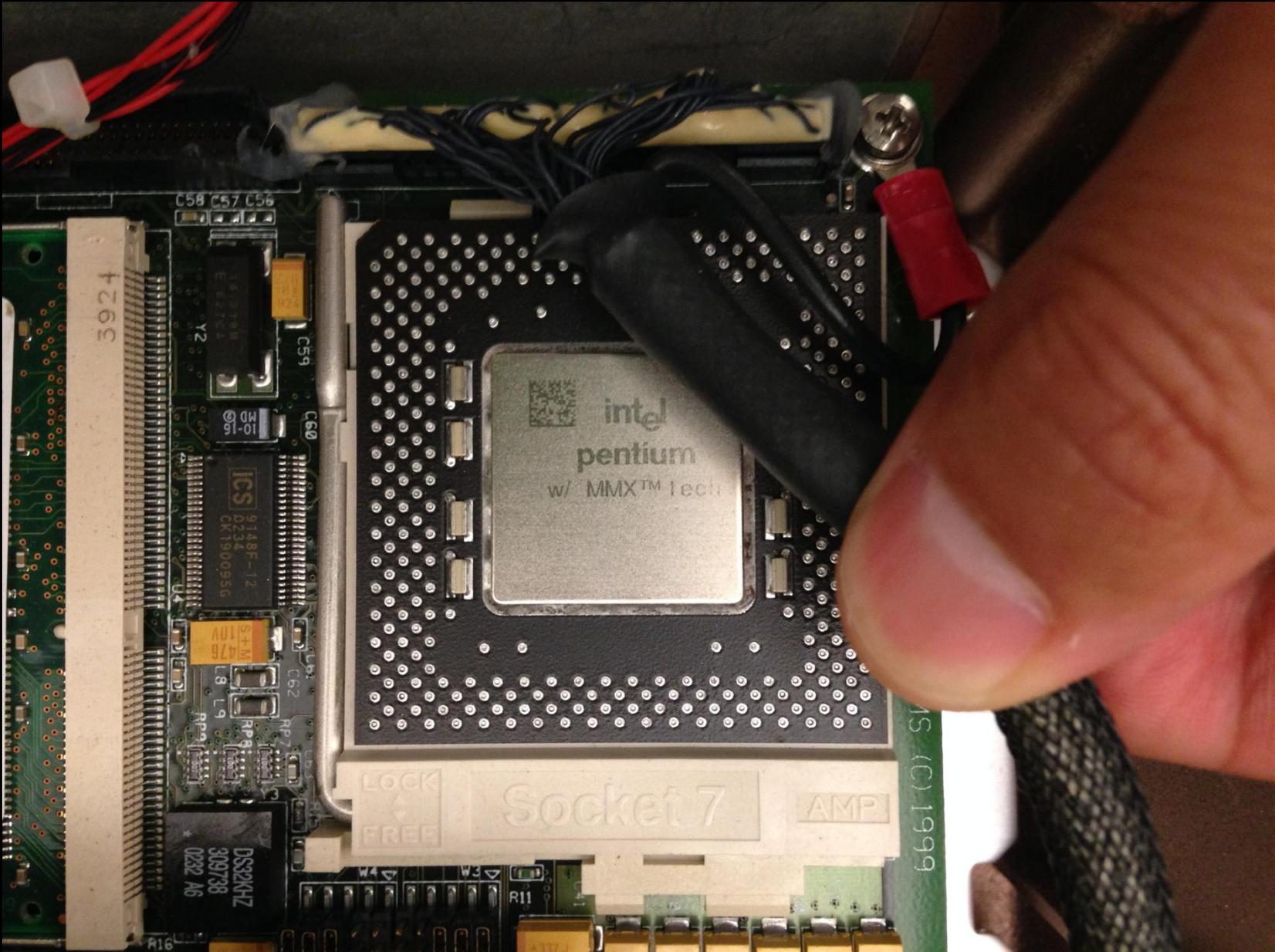
```
.text:00431E10                 xor     eax, eax
.text:00431E12                 and     ecx, 3
.text:00431E15                 rep movsb
.text:00431E17                 mov     edi, offset a695372 ; "695372"
.text:00431E1C                 or      ecx, 0FFFFFFFFh
.text:00431E1F                 repne scasb
.text:00431E21                 not     ecx
.text:00431E23                 sub     edi, ecx
```

Users

Name	Security Level
Operator 1	Operator
Maintenance 1	Maintenance
Administrator 1	Administrator
Super User 1	Super User
D. Hansen	Administrator
J. Eggen	Operator
C. Henke	Administrator
D. Winger	Operator
K. Eckelberg	Administrator
R. Owen	Operator
J. Kempt	Operator

Add | Modify | Delete | Close

Users on the user menu Itemiser

- Operator 1

- Maintenance 1

- Administrator 1

- Super User 1

- <various user accounts>

PROPERTY OF
FEDERAL PRISON SYSTEM

0610 100344

Users in the Binary

- Operator 1

- Maintenance 1

- Administrator 1

- Super User 1

- Administrator 2

- Super User 2

Users in the Binary vs User Menu

Binary

- Operator 1

- Maintenance 1

- Administrator 1

- Super User 1

- Administrator 2

- Super User 2

User Menu

- Operator 1

- Maintenance 1

- Administrator 1

- Super User 1

Two Backdoor Accounts

- Administrator 2: 838635

- SuperUser 2: 695372

Detector Flow Warning

Explosives Mode

Warnings: Press for help

Version 8.17

Super User 2

Clear	Trigger	Help	Menu	Prev. View	Reset View

| Select Scan | Intensity Map | Processed 3D | | Measure | Pan | Zoom |

Users ✕

Units)

Name	Security Level
Operator 1	Operator
Maintenance 1	Maintenance
Administrator 1	Administrator
Super User 1	Super User
D. Hansen	Administrator
J. Eggen	Operator
C.Henke	Administrator
D. Winger	Operator
K. Eckelberg	Administrator
R. Owen	Operator
J. Kempt	Operator

14

Units)

Advisory (ICSA-14-205-01)

Morpho Itemiser 3 Hard-Coded Credential

Original release date: July 24, 2014

🖨 Print   🐦 Tweet   f Send   ➕ Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Independent researchers Billy Rios and Terry McCorkle have identified hard-coded credentials in the Morpho Itemiser 3. Morpho has not produced a patch, update, or new version that mitigates this vulnerability.

MITIGATION

Morpho has decided not to address this vulnerability at this time.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

Blame the vendor?

This is actually, TSA's Fault

- TSA depends on this equipment to do their job

- TSA operators do not have the expertise to detect exploited devices

- TSA has not conducted adequate threat models on how these devices are designed from a cyber security standpoint

- TSA has not audited these devices for even the most basic security issues

- Vendors develop devices to meet TSA requirements

- TSA certifies devices it deems satisfactory

- We pay for all this...

I hope that someone (maybe the GAO?) **trusts** what the TSA is telling us about their devices, but **verifies** the engineering is a reality

If you have embedded devices, I would hope you would do the same for your devices

BEFORE you fork over the $$!

Questions?