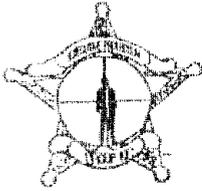*With Allah's Name, The Merciful Benefactor, The Merciful Redeemer*

EXECUTIVE PROTECTION GROUP, INC. (XECPRO, INC.)
EPG XECPRO, INC. INVESTIGATIONS
3131 N Stemmons Freeway, Suite 123, Dallas, TX 75247

(214) 351-0150   (214) 351-0621 fax

PROTECTIVE SERVICES ♦ INTELLIGENCE ♦ ENFORCEMENT ♦ INVESTIGATION

29 July, 2000

Mr. Shukri Abu Baker, C.E.O.
Holy Land Foundation for Relief and Development
504 International Parkway, Suite 509
Richardson, TX 75081

Ofc: (972) 699-9868
Fax (972) 699-0198

Re: Technical Surveillance Countermeasures
Basic RF Sweep Results and Recommendations

Dear Brother Baker:

As-Salaamu-Alaikum. This letter is to thank you and your organization for allowing EPG, Inc. to provide a Basic RF Counter-Surveillance Sweep of your facilities on Wednesday, 23 August, 2000. We were pleased to provide this service at a 50% discount, as a small contribution to your on-going work on behalf of the community. Al-Hamdulilah!

Following please find a Statement of Results for the sweep, as well as information regarding Technical Surveillance Countermeasures and Recommendations for your specific situation.

Brother Baker, thank you again for allowing EPG, Inc. to be of service, and I look forward, insha-allah, to working with you in the near future. Please feel free to contact me at mobile number (214) 662-0265, or office number (214) 351-0150, at your convenience.

Sincerely,
Your brother in service to Allah,

Shihan Dr. F. D. Hale, D.M.
President and C.E.O., EPG, Inc.
Regional Director of Security,
Muslim American Society

ars:DOC
Attachments

HLDL146 0001570

With Allah's Name, The Merciful Benefactor, The Merciful Redeemer

EXECUTIVE PROTECTION GROUP, INC. (XECPRO, INC.)
EPG XECPRO, INC. INVESTIGATIONS
3131 N Stemmons Freeway, Suite 123, Dallas, TX 75247
(214) 351-0150   (214) 351-0621 fax
PROTECTIVE SERVICES ♦ INTELLIGENCE ♦ ENFORCEMENT ♦ INVESTIGATION

Mr. Shukri Abu Baker, C.E.O.
Holy Land Foundation for Relief and Development
504 International Parkway, Suite 509
Richardson, TX 75081

29 July, 2000

Ofc: (972) 699-9868
Fax (972) 699-0198

STATEMENT OF RESULTS

On Wednesday, 23 August, 2000, after the close of normal business hours, Executive Protection Group, Inc. (XECPRO INC.) performed a Technical Surveillance Countermeasures Basic RF Sweep of the Holy Land Foundation for Relief and Development facility located at 504 International Parkway, Suite 509, Richardson, TX 75081.

The Basic RF Counter-Surveillance Sweep determined that certain aspects within the facility, and therefore the Foundation, have been under technical surveillance by unknown entities, for an undetermined period of time. At the time of the sweep, certain recommendations were made regarding these findings, as well as some general suggestions.

Further, EPG, Inc. is still set to provide a second sweep, at no additional charge to the Holy Land Foundation, at a mutually agreeable future date.

Following please find additional information regarding Technical Surveillance and Technical Surveillance Counter Measures. Please also pay particular attention to the cost sheet for performance of various Technical Surveillance Counter Measures; you will note the Foundation has received a more than generous discount for the services rendered.

Sincerely,
Your brother in service to Allah,
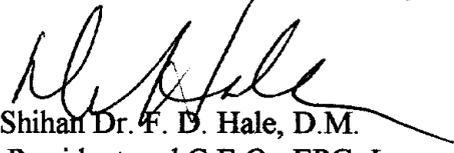
Shihan Dr. F. D. Hale, D.M.
President and C.E.O., EPG, Inc.

ars:DOC
Attachments

2   HLDL146 0001571

What is TSCM, Debugging, Bug Sweeps and Counterintelligence?

THE THREAT - ILLEGAL EAVESDROPPING IN THE UNITED STATES

The manufacture, sale, installation, and monitoring of illegal surveillance devices is a multi-billion underground industry within the United States.

The U. S. State Department estimates that at least 800 million dollars of illegal bugging and eavesdropping equipment is imported and installed into corporations in the United States each year.

The majority of this equipment is illegally imported into the Untied States from France, Germany, Lebanon, Italy, Canada, Israel, England, Japan, Taiwan, South Africa, and a host of other countries.

Additionally, anyone with a soldiering iron and a basic understanding of electronics can build and install an eavesdropping device,. The raw materials to build such a device such as cordless teleph0ones, intercom systems, and televisions.

In the United States over six million dollars worth of surveillance devices are sold to the public each day. Most of these products are sold from storefront operations, spy shops, attorneys, and via private investigators located in major metro areas such as New York, Miami, Los Angeles, San Francisco, Dallas, Chicago, and Minneapolis. This does not include the billions spent each year for legitimate eavesdropping products purchased by law enforcement and military agencies.

This equipment is commonly sold over the counter, via mail order, and through the Internet. Most of these buffing devises cost only a few dollars, but highly sophisticated, quality products may be purchased for less than one thousand dollars.

In New York City alone there are over 85 companies which will not only sell you the eavesdropping device, but will break into the target's office to install the device, and for an additional fee will provide a monitoring and transcription service.

The FBI and federal law enforcement agencies have repeatedly indicated that they lack the resources and training to enforce or properly investigate the technical security threat within the United States.

Technical surveillance and industrial espionage is a serious problem which can have a **VERY GRAVE IMPACT** on your company and your own personal freedoms.

VARIOUS TYPES OF TSCM SERVICES

TSCM - Technical Surveillance Counter Measures

TSCM includes all countermeasures employed to prevent or detect the interception of sensitive, classified, or private information. TSCM is typically an inspection by a technician or engineer of a physical item or place (briefcase, automobile, office, home, boat, etc.). The purpose is to locate possible covert surveillance devices (bugs), technical security weakness, and technical security hazards. A TSCM specialist will also evaluate for weaknesses: all locks, alarms, and other systems of physical and electronic security or controls.

Vulnerability Analysis/Threat Assessment - A formal vulnerability analysis or threat assessment should be performed prior to any TSCM Sweep. The TSCM specialist will normally visit the facility for several days, and identify weaknesses with locks, doors, alarms, fence lines, video cameras, telephone systems, network, and computer security. The end product for a vulnerability analysis is a brief written report with addresses specific issues which need to be corrected.

TSCMFaqs1.doc

The primary purpose of a vulnerability analysis is to answer the following questions:

- **WHO** would want to spy on us?
- **WHAT** information would they be interested in?
- **WHERE** would they attack us?
- **WHEN** are we most vulnerable?
- **HOW** could they attack us?
- **EFFECTS** of our corporate secrets being released?
- **ARE** we as secure as we think, where are we vulnerable?

It's a waste of money to have any TSCM services performed without first having a careful vulnerability analysis or threat assessment completed.

TSCM Inspection - An evaluation, which does not involve test equipment, of a sensitive facility to determine physical security measures required to protect against technical penetration or unaided audio leakage.

IPM: In Place Monitoring - This is the simplest and lowest level of legitimate TSCM sweep. It consists of monitoring a given thing or place while an event or meeting is in progress. IPM assumes that the facilities are secure and that the only threat is from meeting attendees (i.e.: tape recorders, wireless microphones, etc.).

Full TSCM Survey/Sweep - A comprehensive electronic, visual and physical examination of a sensitive facility by TSCM personnel to ascertain that the area is free of technical penetrations and to detect technical security hazards and weaknesses.

This type of inspection is commonly done for attorneys, executives and corporate board rooms. For this inspection every wire in a given area is checked for any type of covert listening or video devices. Special equipment is used to

TSCMFaqs1.doc

search for covert devices transmitting on the airwaves. Normally the RF Sweep is done first, followed by the wire and conductor check, followed by a detailed physical search.

Protective Detail TSCM Survey/Sweep - Performed strictly for high threat situations (heads-of-state, diplomats, VIPs, celebrities, corporate executives, and other wealthy or important people). This is the type of inspection the U.S. Secret Service performs for the President when he is going to be visiting a place. In addition to a full inspection it also involves inspecting and x-raying walls, lamps, furniture, cushions, etc.,

Additionally, this type of inspection also looks for explosives, bombs, poisons, chemical weapons, biological weapons, and other safety and security hazards.

The goal is to locate not only bugging devices, but anything that could cause the protectee any harm or embarrassment.

THE OBJECTIVES OF ANY TSCM PROGRAM OR SERVICE:

Detection: The measures taken to detect technical surveillance devices, technical security hazards, and physical security weaknesses that would permit the technical or physical penetration of a facility.

A technical surveillance device is an item designed to intercept conversations or electronic transmissions and are commonly known as "bugs".

A technical security hazard may allow the unintentional transmission of information, and is any condition which would permit the technical surveillance of an area. This condition may occur with equipment due to its normal design, installation, operation, maintenance, component deterioration, or damaged condition. For example, some telephones have the ability to pass audio even when hung up.

TSCMFaqs1.doc

Nullification: the process of neutralizing or negating technical devices employed by making the placement of such devices more difficult. This includes ensuring that a room is protected with adequate physical construction and security measures, thus making the placement or use of illegal listening devices ineffective.

Isolation: A method to deter, or make extremely difficult, the introduction of an eavesdropping device by establishing special areas, security areas, or SCIF's for the conduct of classified or sensitive activities.

TSCM & COMMON BUGGING

Common Technical Surveillance Devices

Bugging devices may utilize any frequency between DC and light. There are roughly 2,500 popular bugging frequencies used by the various Spy Shops devices around the world. However, be advised that people doing bugging like to stay clustered around certain frequencies.

The device may use the AC power circuits (very popular with federal surveillances), telephone wiring, or HVAC system as the transmission path (15 Hz to 450 MHz+), and may also use spread spectrum technology.

To find FR transmitters an antenna search grid of less then 10 by 10 foot (the size of an average office) should be used. Every cubic centimeter of the facility must be inspected through visual and electronic techniques.

Remember: Bugs are always installed in groups of at least three (3); the one that was easy to find (the fools bug), the one that you'll find if you really work hard (the pro bug), and then the real bug that's almost impossible to find (the spy's bug).

TSCMFaqs1.doc

The only thing on earth that can find a bug is a pair of well trained human eyes, and a set of callused and experienced hands. The electronic test equipment is only used to suggest to the inspector where to look.

There are no magical black boxes that find bugs.

All phone rooms, riser closets, demarcation points, and boots, must all be checked for tampering and electromagnetic anomalies (RF activity).

All electrical outlets, light fixtures and switches, circuit breakers, distribution boxes, electric meters, and transformers must be checked for tampering and electromagnetic anomalies (RF activity). The transformer and circuit breaker panel is the most important of these, as it's commonly modified to facilitate technical surveillance.

The microphone or video camera may be hundreds of feet away from the transmitter or recorder, so be sure to check all potential transmission paths.

TSCMFaqs1.doc

Phone Bugging and Modifications

If you are reading this then you probably have a telephone, and if you have a telephone you already have an excellent bugging device installed in your home or office.

In many cases nothing has to be done to the telephone (i.e.: Northern Telcom) to turn it into an excellent room bug, but in most cases a simple capacitor (at a cost of three cents) can be installed and a wire snipped to turn your telephone into a very high quality eavesdropping device.

Telephone have microphones, speakers, ringers, microphonic transducers, and power which provides everything an eavesdropper needs to listen in on your business or personal affairs.

What follows are a few of the hundreds of things an eavesdropper can do to turn a telephone into an excellent surveillance device.

Native or Friendly Threats

Cellular and cordless telephones by their very nature emit large amounts of RF energy which may then be intercepted at fairly large distances. Even the new "secure" digital spread spectrum telephones may be easily intercepted with only a few dollars of parts available at any Radio Shack.

Many Modems, telephones and speakerphones also emit RF energy when in use, this energy may then be easily intercepted by an eavesdropper using inexpensive radio receivers.

The speaker phone systems made by Lucent, Panasonic, U.S. Robotics, and others have a history of "native emissions". One of these phones ordered right from the factory, with no modifications, will often transmit RF energy which may

be easily intercepted several hundred feet away. For example, many of the Merlin speakerphones emit an RF (NFM) signal around 300-MHz.

Many data modems (Practical Peripheral, Motorola, Rockwell, etc.) also transmit RF energy when in normal use. This allows an eavesdropper to easily intercept and record the signal at considerable distance. Often all that is needed to monitor the signal is a modified twenty dollar FM radio. For example, an unmodified Practical Peripheral 28.8 modem transmits an RF signal in the 120-130MHz range, the signal is wide FM modulated, with several pulse modulated components.

Fax machines may also do this, when a confidential document is sent to your client, you may also be broadcasting it to an eavesdropper. This is a serious problem with Sharp, Canon, HP, and other fax machines.

RF Transmitter

This is the classic phone bug, a small RF transmitter is attached to the phone line somewhere outside the facility. Power may be supplied by the current already on the phone line or from a small battery. Most devices of this nature only transmit when the phone is lifted off of the switch.

RF Transmitter with Microphone

This is similar to the above device, but it has its own microphone, and is typically installed inside the telephone. Such a device is normally considered a room bug. This type of device transmits an RF signal over the phone or power lines (9kHz to 750 kHz is common, but the signal may be as high as 450+ MHz).

Infinity Transmitter or Harmonica Bug

An older devices, which is attached to a telephone, and when called from an outside telephone would enable the caller to listen in on room audio.

Recorder Starter/Drop Out Relay

TSCMFaqs2.doc -
Phone Bugging and Modifications

This is little more than a device that detects the voltage or current change caused when the handset is lifted off of the hook. Its purpose is to activate a tape recorder hidden nearby. Some recorder starter devices may also detect sound, and activate if sound is detected on the line.

This type of device is popular with private investigators and "Walter Mitty wanna-be spies". The product may be purchased at Radio Shack or other electronics stores for under twenty dollars.

Slave or Bypass Device

This type of device provides electrical isolation between a target line and an eavesdropper, which provides a low level of security against detection (popular with law enforcement).

CO/REMOBS Monitoring (Central Office Remote Observance)

Allows the phone company or government to legally tap or monitor your phone. The computer that handles phone service to your local area is instructed to transmit a digital copy of all of you calls to a secure listening post (which can be located anywhere in the world).

All that is required to do this is access to the ESS translation, and a T-Carrier or OC-xx data line (a normal "loop" line is rarely used). With a 622 mb fiber optic line eavesdropping can easily access, and listen in on over 11,100 lines at a time in a local area.

This function of the phone system is very loosely controlled as the maintenance people at the phone company use it for routine maintenance. Any computer hacker or Phreaker can easily access the system. Private investigators and insurance companies have also been known to illegally use this system to gather information on targets.

Hookswitch Bypass Methods

TSCMFaqs2.doc -
Phone Bugging and Modifications

Inside the telephone is a switch that disconnects and shorts out the microphone in your telephone handset when the telephone is hung up (hookswitch). If the telephone circuitry is slightly modified (cut one wire and then installed a three cent part) the microphone will be "hot" all the time. If the microphone is hot all the time, then the eavesdropper can go anywhere outside that area; plug an audio amplifier into the phone line; and get excellent quality room audio. It is effectively the same as installing a microphone or eavesdropping device in the room or building.

Several telephone systems lack a hookswitch mute circuit (such as the cheaper phones made by Northern Telcom, Toshiba, and several others). This allows an eavesdropper to perform a technical surveillance without actually gaining access to the area (such as a hotel room) or performing any type of modification to the telephone.

TSCMFaqs2.doc -
Phone Bugging and Modifications

12

Types of Wiretaps, Bugs and Methods

WIRETAPPING

Wiretapping is the preferred method of obtaining intelligence, for quality reasons. It involves tying into a wire that is used for communication by the target. This wire can be a telephone line, a PBX cable, a local area network, a video system, or an alarm system.

The goal in a wiretapping is to secure high quality information, and to minimize the possibility of the eavesdropping being detected.

Wiretaps are broken into four categories: Hard, Soft, Record, and Transmit.

A Hard Wiretap

A hard wiretap is when physical access is gained to a section of wire that the signal (i.e.: telephone line) travels on. A second set of wires is attached, normally through the use of an isolation or slave device. The signal is then bridged back to a secure location. this type of wiretap is very popular with law enforcement, but is usually outside the scope of most eavesdroppers.

A Soft Wiretap

A soft wiretap is a modification to the software used to run the phone system This can be done at the telephone company, or in the case of a business, the PBX. A soft wiretap is a preferred method to tap a phone, is easy to catch on PBX, but tough to find in the telephone company's system. (It is sometimes called a REMOBS ESS or translation tap.) This type of tap is very popular with large law enforcement agencies, larger corporations, and with hackers who find it quite simple to gain access via maintenance software.

13

A Record Wiretap

A record wiretap is nothing more than a tape recorder wired into the phone line, very easy to find on a TSCM inspection. Similar to a hard wiretap, but the tapes must be changed on a regular basis. This is very, very popular with amateur spys, and private investigators.

A Transmit Wiretap

A transmit wiretap is an RF transmitter (or 'Bug") connected to the wire and will be covered in detail below. This type of tape is also very popular, but the RF energy it produces radically increase the chance that it will be detected.

Wiretaps are extremely difficult to detect if properly installed, and require a very high level of expertise, and a great deal of equipment to locate.

BUGGING (EVERYBODY'S FAVORITE SUBJECT)

A "BUG" is a device which is placed in an area which then intercepts communications and transmits them out of that area to a listening post.

There are five categories of "Bugs": Acoustic, Ultrasonic, RF, Optical, and Hybrid.

Acoustic is the placing of a water glass, stethoscope, or rubber tube into an area and directly intercepting the communication with the naked ear.

Ultrasonic is a technique to convert the sound into an audio signal above the range of human hearing, the ultrasonic sonic then intercepted nearby and converted back to audio.

RF, or Radio Frequency, is the most well known type of bugging device. A radio transmitter is placed in an area or in a device. This is y0our classic martini olive bug and " spy shop" store device. Extremely easy to detect, but cheap, disposable, and difficult to trace back to the person who planted it. (This was the Watergate bug.)

TSCMFaqs3.doc -
Wiretaps, Bugs and Methods

Optical is a bugging device that converts sound or data into an optical pulse of light. It is rarely used, expensive, and easy to detect.

Hybrid is any combination of the above techniques and devices to make a customized hybrid bug.

FAMILIES OF BUGS

Free Space Emission:
1. Acoustic/Audible Pressure Waves
2. Acoustic/Ultrasonic Pressure Waves
3. Optical/Invisible Light (UV, etc.)
4. Optical/Visible Light
5. Optical/Invisible Light (Infrared, etc.)

6. RF Transmission (VLF) 3 kHz - 3 MHz
7. RF Transmission (HF) 100 kHz - 70 MHz
8. RF Transmission (VHF) 30 MHz - 300 MHz
9. RF Transmission (UHF) 300 MHz - 1 GHz
10. RF Transmission (Microwave Low) 900 MHz - 3 GHz
11. RF Transmission (Microwave Mid) 3 GHz - 12.5 GHz
12. RF Transmission (Microwave High) 12.5 GHz - 26.5/33/40 GHz
13. RF Transmission (Microwave mm) 26.5/33/40 GHz - 325 GHz
14. RF Transmission (Microwave mm2) 325 GHz - 1.5 THz

15. Free Space - Magnetic

Conducted Emission:
16. Audible (Voice Frequency)
17. Ultrasonic
18. Video
19. Current Carrier up to 500 kHz (AC mains, Phone, CATV, etc.)
20. Radio Frequency (AC/Mains Devices, waveguide, etc.)
21. Fiber Optic
22. Other

TSCMFaqs3.doc -
Wiretaps, Bugs and Methods

TYPES OF COVERT EAVESDROPPING ACTIVITIES

Intelligence:

1. Counter Counter Intelligence (Counter-TSCM)
2. Counter Intelligence (TSCM)
3. Active (Classic spying, Heavy Bugging, and Black Bag Jobs)
4. Passive (Primarily Listening, Minor Bugging)

Law Enforcement:

1. High Level Intelligence (Domestic - DEA, FBI, USSS, FISA, etc.)
2. Low Level Intelligence (Domestic Law Enforcement)
3. Investigation of Major Crimes (Murder, Arson, etc.)
4. Active (Wiretaps, Body wires, etc.)
5. Passive (Cellular Phone/Beeper Monitoring)
6. Tactical (SWAT Teams, Throw-Phones, etc.)
7. Management (Video in Police Cars, Wireless Microphones)
8. Outlaw (Illegal Surveillance Activities)

Private Investigator:

1. Intelligence - Active (Black Bag Jobs)
2. Intelligence - Passive (Cellular Phone/Beeper Monitoring)
3. Surveillance - Active (Black Bag Jobs)
4. Surveillance - Passive (Cellular Phone/Beeper Monitoring)

Amateur/Private Individual:

1. Intelligence - Active
2. Intelligence - Passive
3. Surveillance - Active
4. Surveillance - Passive

TSCMFaqs3.doc -
Wiretaps, Bugs and Methods