HIGHPOINT SECURITY
TECHNOLOGIES Inc.

Criteria for Selecting a Company to Conduct a Technical Security Inspection

Highpoint Document

2006

CRITERIA FOR SELECTION OF A COMPANY TO CARRY OUT A TECHNICAL INSPECTION PROJECT

1. The Company must have the ability to carry out a thorough on site analysis of the project and to provide management of the client organization with a comprehensive plan, including an estimate of the time it will take to conduct, as well as the cost of conducting the project. The plan should provide for both an electronic and physical inspection. The plan should also provide for the submission of a report at the conclusion of the project.

2. The Company providing the team(s) must have access to persons of varied technical and other backgrounds which will allow it to provide a team (or teams) comprising skills appropriate to the project.

3. The Company must be prepared to provide a resume for each member of the team(s) as well as documentation relative to their training. In addition, the Company must be prepared to certify that it has carried out a background check on team members and show that they are bondable.

4. The Company must possess, or have access to, various physical and electronic equipment that will enable its team(s) to detect Technical Intrusion attacks using the following approaches and methods:
    - direct observation equipment (tools, ladders, search scopes, etc.)
    - telephone , telex and data line analysis
    - power line carrier analysis
    - cable and CCTV cable analysis
    - automated receiver searching
    - spectrum analysis
    - spectrum monitoring
    - non-linear junction detection
    - X-ray inspection(access only, when required)
    - thermal imaging.

5. The Company must possess or have access to equipment that can detect, locate and neutralize surveillance devices e.g. a tape recorder, hard-wired microphones, video cameras, hidden microphones in telephones, radio-frequency transmitters, optical (fiber) connected monitoring devices, intrusive devices using various domestic or industrial equipment cables to relay the information and passive/reflective acoustic devices. Further, if the situation so warrants the Company must have access to a person skilled in the installation of permenant counter-surveillance devices.

6. The report submitted by the Company on completion of the project must summarize the project objectives, the methodology used, the presence or absence of electronic surveillance devices, counter surveillance recommended (including equipment needed), training required by the client's security organization and changes recommended in the client's security policies and practices.

Technical Discussion

Equipment used by the Company must have minimum characteristics that will permit the detection of the most modern attack methods, methods previously used to attack a premises and equipment that may or may not be turned on at the time of the technical inspection. This should include:

- Receiver(s) with the ability to detect an RF signal in AM, FM, WIDE FM, SSB (upper and lower side band), Frequency Hoppers, CW, FSK and other techniques currently used in sophisticated intrusion devices. The receiver must have the selectivity, sensitivity and stability of current receivers used in sweeping (e.g. ICOM, Watkins Johnson, ACR, Scan-lock, etc.)
- A non-linear junction detector to detect harmonic anomalies.
- A system for identifying differential radio frequency field gradients.
- A spectrum analyzer with the capability of sweeping to at least 12 GHz.
- An oscilloscope of suitable good quality with a capability of reaching the lowest frequency of the spectrum analyzer.
- Good quality test and analytical equipment to sweep power lines and telephones, together with other like communication, alarm or video systems.
- Auxiliary and ancillary equipment used in the sweeping community, such as TDR equipment, multi-meters, audio amplifiers, thermal imagers etc. General hand tools and an electronics tool kit are also required.

Staff performing a Technical Security Inspection must be qualified to a combined standard of: a Professional or Graduate Engineer; an Electronics Technologist; an experienced Technician with considerable experience in the legal installation of technical intrusion equipment, intensive training by a recognized CTI training institution. They must possess a firm grasp of the principles of radio communication, data communication and telephony. Experience should show a minimum of 3 years in Governmental/Military or Private Industry duties related to the field. This experience will give them the capacity to electronically and physically .

- find hard wire or quick plant microphones, power line carriers etc.
- find and prevent attacks of customer alarm, video, audio and network systems.
- check all types of cables, fibers, telephone sets, computer equipment and any other devices that may lend them to a technical attack.
- recognize digital microphone, noise masked, tone masked, frequency hopping and spread spectrum emanations and/or combinations of the above.
- Test for and recommend methods of preventing infra-red, laser, microwave, or like attacks on windows, etc..
- be aware of, sweep for, and recommend prevention of Tempest, EMI and RFI attacks.