Executive Summary

The use of short range optical wireless, particularly on Election Day should not be allowed because:

1) It is impossible to ensure that only Election Officials will be able to communicate with voting systems using the optical link.

2) Slow Infrared (SIR) optical communications like other transmission media allow the exchange of software, data and control information at a relatively high data rate of 115,200 bits per second.

3) Because the communicating devices have no physical connection, and the radiation is invisible, it is impossible to determine in a election environment if there are unauthorized devices communicating with the voting system.

4) Even if the unauthorized device did not communicate with the voting systems, it would still be possible to "listen", intercepting anything transmitted between authorized devices.

5) Anyone with an optical device operating on the same wavelength can interfere with the authorized optical transmissions. As a minimum this could be disruptive to the voting process.

6) Any IrDA device supporting the upper level protocols can easily communicate with the voting systems if the information is not encrypted.

7) The use of wireless (or any communications methods) on Election Day adds substantial additional risk that this communications path can be exploited to change the functioning of the voting equipment after Logic and Accuracy Test (LAT) are complete.

8) While safety issues with infrared are a topic of significant discussion, and one that warrants an in depth study if the technology is to be deployed in polling places, every day use of these devices have decreased awareness of the potential dangers they pose. The power levels should be strictly regulated if the technology is placed in public poling places.[1]

It is also impossible to verify that the software in voting system performs only authorized functions and cannot be corrupted using various attacks (e.g., buffer overflow). If the communicating devices are tethered the ability to communicate with external units are at least restricted to other devices physically attached to the network.

Networked voting systems are appropriate only for pre-election preparation of voting machines. All voting systems should be disconnected from any network prior to LAT and until election results are complete. After preparation for the election is complete, and prior to LAT voting systems should be isolated to the fullest extent possible from communications networks of any kind. Only the voter user interface (and then only for voting) should be used to interact with the voting system. This isolation should be retained until the election results are settled and all recounts (if any) are complete.

---

[1] Infrared Data Association Serial Infrared Physical Layer Link Specification http://web.mit.edu/rec/iap/mirror/irda/IrPHY_1_2.PDF

Wireless, what is it?

Simply put, wireless is any communications method that does not depend on wires (metallic or fiber) for the transmission of communications signals. Wireless communications provides "connectivity" between two or more devices (a transmitter and a receiver) enabling them to exchange information. The fundamental difference between wireless communication and other "wired" forms of communications is the medium over which the encoded energy containing information is transferred between the transmitter and receiver. In wireless systems energy transfer occurs through air or through free space without a physical connection between the devices. The energy transfer can be visible optical radiation, invisible infrared, ultraviolet or radio frequency (RF) to name a few.

The energy transferred between the two devices can follow a narrow path, essentially a straight line between origin (transmitter) and destination (receiver) – line of sight (LOS), and a diverging path or be sent out in all directions (omni directional). The radiated energy behaves in different ways depending on its frequency. Higher frequency signals such as light (optical) tend to be more directional whereas RF signal tend to be transmitted in all directions without the use of specially designed directional antennas. Another characteristic of the energy transmitted is its ability to penetrate solid objects. Optical signals do not penetrate solid objects unless they are transparent to that frequency of radiation, whereas RF signals (at lower frequencies) can flow freely through or around solid objects such as walls. Both optical and RF signals can bounce off various surfaces form walls, water, mirrors and buildings.

The distance both types of signals can travel and still be capable of being recovered by the receiver depends on the medium the signal travels through and the strength of the signal (amount of energy originally transmitted) and the sensitivity of the receiver. In general the signals become weaker the farther they go. It is clear that each type of signals is affected greatly by the environment that is traversed between the transmitter and the receiver. Optical signals would be confined to a room if there are no transparent walls (windows) or open doors, whereas RF signals would not.

The main advantage of IrDA, is that communications can be established without having to deploy wiring or cables. This advantage also applies for RF technologies such as Bluetooth. For optimal operation, IrDA requires an unobstructed Line of Sight (LoS) path from the transmitter to the receiver. A ceiling mounted access point generally provides such a path, with the access point typically connected to a wire or cable based LAN.

What is IrDA

IrDA (**I**nfra**r**ed **D**ata **A**ssociation) is a standard defined by the IrDA Consortium. It specifies a method to wirelessly transfer data via infrared radiation. The concept of short range optical networking is simple. Imagine a standard fiber-optic cable based network link between two devices, then remove the cable and replace it with a line-of-sight IR beam that travels between a pair of transmitter-receivers.

IrDA Control

IrDA Control provides a suite of protocols that peripherals such as keyboards, joysticks, mouse, and pointing devices can use for communicating with a host computer. IrDA Control includes:

- **IrDA Control PHY (physical):**

  IrDA-Control-PHY provides bidirectional and error-correcting data transmission at speeds of up to 75 Kbps over distances of up 16 feet.

- **IrDA Control MAC (media access control):**

  IrDA-Control-MAC enables host devices to communicate with up to eight peripherals simultaneously.

- **IrDA Control LLC (logical link control):**

  IrDA-Control-LLC handles frame sequencing and error control (retransmission of data when errors occur).

IrDA-Data

IrDA-Data is designed for two-way point-to-point communication at speeds of up to 4 megabits per second (Mbps). IrDA Data can be used for communication between palm computers, digital cameras, cellular phones, and other devices. IrDA Data includes the following protocols:

- **IrDA Data PHY (physical) layer:**

  IrDA-Data-PHY provides bidirectional error-correcting operation from 9600 bits per second (bps) up to 4 Mbps over distances of at least 3.3 feet (1 meter). Specifically, asynchronous serial transmission is supported between 9600 bps and 115.2 kilobits per second (Kbps), synchronous serial transmission at 1.152 Mbps, and synchronous communication at 4 Mbps.

- **IrDA Data Infrared Link Access Protocol (IrLAP):**

  IrLAP is a serial link protocol adapted from the High-level Data Link Control (HDLC) protocol. IrLAP provides a single serial connection between two IrDA devices and manages the device-to-device discovery, connection, and reliable data transfer functions.

- **IrDA Data Infrared Link Management Protocol (IrLMP):**

IrLMP is used for link control and multiplexing of IrDA devices. IrLMP allows multiple IrDA devices to communicate over a single infrared link and provides for protocol and service discovery through the Information Access Service (IAS).

Acronym	Meaning	Data Rate
SIR	Slow infrared	9.6 kbps to 115.2 kbps
MIR	Medium infrared	576 kbps and 1152 kbps
IR	Fast infrared	4 Mbps
VFIR	Very fast infrared	16 Mbps

How far can optical wireless devices transmit signals?

Theoretically using optical, the transmission distance is limited only by the output power of the source and the sensitivity of the detector. With a suitably sensitive detector, optical radiations from planets orbiting stars in other solar systems have been detected. Therefore in theory a transceivers could be designed to operate at the proper power level and communicating with a high gain receiver could operate over any desired distance.

Form a practical standpoint however, when using Devices conforming to Short-Range IrDA Data Physical Layer specifications standard [IrDA 1.0 and 1.1] distances are limited to 1.0 meter (~3.3 feet). At this distance devices provide near error free (1 error bit in 10^9 bits transmitted) communication at a data rate of 115.2 Kb/s or over 14,000; 8-bit characters per second plus overhead. Directional transmitters (IR LEDs) exist for transmitting at longer distances up to 30 or 40 ft.

Using IrDA-Control-PHY devices can transmit at 75 Kbps up to 16ft. There are manufacturers that offer cradles for IrDA devices like PDAs that allow them to operate over extended distances. A transceiver manufactured by Optical Paths support distances of over 100 feet at data rates up to 115kbps. Later generation of their products will support distance of up to 500 feet using the IrDA v1.1 / Fast Infrared specification allowing transmissions at 4.Mb/s. Under the existing NIST/IEEE P1583 specifications a manufacturer could install a system capable of operating at these extended distances as no maximum distance or power setting is stated.

Because most IrDA devices use standard protocols at the upper layer (TCP/IP), it can easily be interconnected with other networks. All of the voting terminals in a room could be added to a Local Area Network (LAN) by mounting an optical transceiver node in the ceiling that is capable of communicating with each of the voting terminals. This would be difficult to monitor and control if the optical node on the LAN was there for other approved reasons. Determining whether the node was disabled and could not communicate over the LAN would be difficult to determine, even by a trained observer without close inspection. The only easy solution would be to mandate that the ceiling mounted node have an opaque cover while voting. Precautions such as these are not mandated in the NIST standard.

Infrared optical links used in the Diebold system are based on the Infrared Data Association (IrDA) specification and currently operate at up to 115.2 K bit/s. The Windows CE Operating System implements Microsoft's TCP/IP protocol stack.

Are there Eye Safety issues with IrDA?

"Short Rang" optical devices under P1583 are not required to comply with IrDA Class 1 device specifications. The IrDA specifications indicate that the range of IrDA devices has been limited to 1m for reasons of eye safety.

Infrared (IR) light emitted by IrDA compliant devices, at peak power emits at about 300mW using an IR LED. If directional LED or solid state lasers are used an operator would looks directly at the emitter on the TS terminal (required when pointing the control unit at the terminal), thus being exposed to a higher level of IR radiation over a longer period of time.

The focusing property of the eye causes it to concentrate power in the 400 – 1400 nm range, potentially damaging the retina. IrDA devices transmit in the infrared portion of the spectrum (875 nm), and is not visible to the unaided eye. HP's specification for their OmniBook 800 notebook computer recommends not looking directly at the LED emitter.

Because compliance is not mandated in the NIST/IEEE specifications, the power level could be increased by the manufacturer to allow Election Officials the convenience of using the devices at a longer distance.

Should all voting terminals equipped with IrDA ports be required to be placed in windowless rooms?

IrDA devices are typically designed for use in line of sight applications. Because of the nature of infrared light, it penetrates glass or other transparent objects and reflects off walls, ceiling, mirrors and other surfaces. It is possible for signals to be exchanged between two devices that are not in direct line of sight and from a device that is outside of the room.

Note that even if the voting terminal's transceiver was IrDA compliant the remote would not have to comply in either transmitted power or receiver [signal strength] sensitivity. Using such a device the voting terminal could be communicated with from extended distances.

The principal justification for treating short range optical different from radio frequency wireless was to protect against these remote threats from outside the poling place. In an open space, or a room with windows, optical is just as venerable as RF.

Certainly it could be argued that the signal could be encrypted to prevent outside users from communicating with the machine. The same arguments were made for RF and found insufficient. This is why their use on Election Day has been prohibited. Unless windowless polling places with non reflecting walls are mandated similar threats exist with optical.

Will direct line-or-sight paths be required in the precinct between the voting terminal and the Register Judge?
Because IR devices are line-of-sight, a clear unobstructed path is required between the transmitter and the receiver. Unless the Election Official is seated close to the machine being communicated with they will have to either move or clear voters to make an unobstructed path. This would seem to eliminate any convenience the official would derive from using short range optical. The only obvious solution to this is to raise power levels such that reflected signals would still reach the receivers.
Operating multiple devices concurrently in the same room would cause some signal interference if the controllers are pointed in the same direction. This will increase the error rate, requiring either the power level to be increased or the distance to be shortened.

Infrared is unregulated
The infrared portion of the spectrum is unregulated meaning devices can be designed and built to any standard the manufacturer chooses, unlike RF which is regulated by the FCC. For practical (availability of inexpensive components) most manufacturers choose IrDA or the TV IR remote standard.

The infrared beam spreads as it traverses the distance between the transmitter and the receiver. Visualize a flashlight beam that is narrow at the flashlight, but can spread to illuminate a large radius at a distance (this may be aided by a lens). Infrared like the visible light emitted by a flashlight also spreads only slightly more so because of its longer wavelength when uncorrected. IrDA uses a 30^{o} cone for its transmissions. To maximize radiation delivered to the receiver, the beam is directed requiring the source to be pointed at the detector one wants to communicate with.

How Secure is IrDA
IrDA does not provide encryption at the Physical Layer, and depends on the end systems to implement security if any. It is possible for the radiation emitted form the voting terminal or the Election Judge's controller to be intercepted and listened to. Bluetooth, a short range RF technology whose use is restricted by P1583 (as well it should) provides encryption at the physical layer and thus its basic design offers more security than short range optical. The current NIST standard does not mandate link encryption and strong authentication, thus facilitating this kind of attack.

With optical, it is possible for a session to be 'hijacked' unless strong authentication measures are implemented between communicating systems. When a session is hijacked, a foreign device masquerades as a trusted system that is authorized to exchange data. Because the system has no way to distinguish the masquerader from the authorized system, it will accept anything from it as if was authorized.

IrDA Software

IrDA software drivers are available form a number of sources for use with UNIX, Windows and other Operating Systems (OS). Most versions of MS Windows come with support for IrDA already included. This is true of the MS Windows CE operating system as well as Windows XP. Microsoft also provides a free IrDA driver which can be

downloaded from it web site. Other suppliers of IrDA systems (e.g., Ericsson) offer their own drivers including source code (Texas Inurnments).

With the source code available, an interrupt handler (executable code) could easily be added. For example, when the voting terminal receives a special bit configuration (caused by holding down multiple keys concurrently) that is outside the usually accepted range, a special interrupt could be generated invoking a handler that could be programmed to perform any desired function. This would require a small amount of code and could easily be hidden; such code would be difficult to discover.

If such code was installed in the driver, which is considered to be Commercial-Off-The-Shelf (COTS) [even if compiled and installed by the voting system manufacturer] it would not be examined by the ITAs.

Code in such a handler could be designed to place the voting terminal in a mode where it downloads and install an executable module, thus allowing unapproved logic to be added to the voting machine while in use on Election Day. Obviously this executable could perform any function the programmer desired including deleting itself when finished. The only recourse is to disallow communications with the voting terminal during use. It might be augured that such code could be added the day before Election Day. If all software in the system is required to self authenticate using a digital signature these kinds of changes would be detected.

In the Microsoft environment, writing a programming to use the IrDA interface is designed to be simple and straightforward using Windows IrSock. This software is simple to program and operates like any other serial port when using the lower speed version (SIR). Higher speed versions of IrDA will communicate over high speed Ethernet ports as serial ports are usually limited to 115.2 Kb/s.
In some versions of the OS IrDA is Plug-and-Play. This means that when the operating system “boots up”, if it detects the presence of an IrDA device, it will automatically install the driver software required for communicating with it. This means Election Officials would have to take action to disable the device; a procedure that most officials would be unfamiliar with.

Microsoft Statement on the security of IrDA

Microsoft Windows 2000 provides support for infrared-based connectivity. This support is provided through protocols developed by the Infrared Data Association (IrDA). Because of this, they are often called IrDA devices. These devices can be used to share files and printers with other IrDA-device capable systems. The software that handles IrDA devices in Windows 2000 contains an unchecked buffer in the code that handles certain IrDA packets.

A security vulnerability results because it is possible for a malicious user to send a specially crafted IrDA packet to the victim's system. This could enable the attacker to conduct a buffer overflow attack and cause an access violation on the system, forcing a reboot.

What characteristics of IrDA make it different from FR communications?

Presumably there are substantial differences between the two types of communication that warrant an exception for infrared but not for short range radio frequency communications technologies. The justification for this exception is flawed because any differences that matter for secure operation in a polling place are not mandated.

While there are differences between short range optical and radio frequency transmissions, the differences are insignificant in voting system applications. The primary differences are at the physical layer and include:

- The ability of RF to penetrate solid objects allows signals from outside the polling place to be received by a voting terminal; unless polling places are windowless IR radiation could be received from outside the polling place.
- IR is highly directional while RF tends to be omni-directional. While IR is directional, it reflects from smooth surfaces including walls and ceilings.
- IR is not as easily intercepted as RF. Unless the detector receives reflected energy, an interceptor would have to be in line of sight. In most polling environments, reflected energy would not be suppressed thus eliminating this advantage.
- RF devices are strictly regulated and IR is not. Being unregulated, the characteristics and range of IR devices can be set as desired without violating any law or regulation.
- IR devices will be subjected to interference as will RF devices as IrDA becomes more widely used in cell phones, PDA and other devices.

In almost all other aspects, IrDA and RF are more similar than they are different.
The power level of RF devices can be reduced so that they operate only over short ranges (1 meter) specified for IrDA or IR devices can be increased in power level so they operate over longer distances if desired.

While IR devices can be designed to be highly directional, the 30 degree cone specified with IrDA means the signal sill spread if there is significant distance between the transmitter and receiver. A highly directional implementation would require more precise pointing thus limiting the usefulness in a polling place. The fact that infrared radiation reflects off surfaces also means that some of the benefits of its directional nature are lost.

The same upper layer communications protocols can be used with either an IR or RF physical layer. They can both be easily added as nodes on a LAN.

Will other optical devices have to be banned from polling places?

As IrDa becomes more widely deployed, it will be used in cell phones, PDA, watches and other devices. These devices may operate in the same portions of the spectrum as voting system and thus become a source of interference. Even if they do not pass intelligible signals to the voting device (which could occur if the same protocol is also used and the signals are not encrypted) they will interfere with the signals being exchanged between voting system causing an increase in the bit error rate.