Security Tip #12: Restricting Electronic Devices in Federal Courthouses

Public access to cell phones and other electronic devices in federal courthouses pose a host of security-related issues. The United States Marshals Service urges all federal courthouses to adopt a firmly-enforced policy prohibiting persons other than court personnel from bringing electronic devices into the courthouse environment without prior authorization. While inconvenient for attorneys and litigants, such policy is justified and well-reasoned.

Cell phones, smart watches, and computers can be used to record proceedings or surreptitiously photograph witnesses, jurors, and court personnel. In high-threat trials, particularly those involving gangs or criminal networks, such photographs have been employed to intimidate cooperating witnesses and their families. In some cases, it has facilitated retribution. Smart phone technology, which may include streaming videos, also enables real-time communication with criminal associates outside the immediate courthouse perimeter. Such information has obvious strategic value to confederates plotting a security breach. If equipped with encryption capability, such devices may permit transmission of courtroom activity or security staffing with minimal risk of detection.

An additional danger posed by cell phones is their potential use as a remote detonating device for concealed explosives. So-called cell phone triggers have long been the method of choice for terrorists to initiate explosive attacks in Iraq and Afghanistan. Nationwide, electronic device policies differ widely in federal courthouses from minimal restrictions to almost total exclusion. Obviously, a significant consideration is the evolving use of cell phones and computers by attorneys and litigants for information storage. To accommodate known members of the bar and properly credentialed federal agents, some courts grant standing authorization to bring electronic devices into the courthouse while others require case-by-case approval.

In consultation with the Marshals Service, federal courts are increasingly adopting a strict policy of electronic device exclusion in the absence of written court authorization. While each court must develop its security policy based upon its perceived needs, judges should be mindful that potential assailants, often bearing false documentation, are difficult to identify. Furthermore, it is virtually impossible from external observation

to determine whether a cell phone has been programmed to detonate an explosive device.

If your courthouse does not have an electronic device policy, isn't it time to give one some thought?

Security Committee
Federal Judges Association