

Computer Crimes in the Federal Workplace

The number of computers and technology-related devices has increased exponentially in the Federal workplace and these devices have become an indispensable part of our daily work routine. Less than twenty years ago, a personal computer (PC) was a luxury reserved for high-ranking officers and civilians. Now, virtually every employee has a PC on his or her desk, or has access to one. Moreover, the advent of communications technologies such as pagers, cell phones, e-mail and the Internet have provided us with the unprecedented ability to communicate instantaneously and efficiently with people over vast distances.

While communications technology and computer usage has expanded the way in which business is done, at the same time the explosive growth in computer usage has brought along with it a wide range of problems and concerns. The unique nature of the computer and more particularly the Internet, is such that the ability to commit certain crimes has actually increased. The ability of an individual to use the Internet to maintain anonymity has increasingly made it the medium of choice for those seeking to commit crimes, or use this technological marvel for other unauthorized purposes. The use of the computer and the Internet for illegal purposes can be generally grouped into a category of crimes known as computer or cyber crimes. This type of crime involves the use of technologies, including but not limited to, the computer and the Internet to target other computers, persons, and property. Many of these cyber crimes are simply new variations on old crimes.

Federal computer crimes are covered by Section 1030 of Title 18 of the United States Code (18 U.S.C. §1030). This statute first became law in 1984. While other Federal laws relate to the criminal use of computers and technology, this law is designed specifically to address the unauthorized use of computers as well as the information that they contain. Some examples of computer crimes that Federal employees should be aware of are the following:

Transmission of Classified and/or Sensitive Information

Only individuals with proper authorization may access information stored on Federal Government computers. Often this information contains personal data protected by the Privacy Act or material that is vital to national security. Federal law (18 U.S.C. §1030(a)(3)) makes it a crime for anyone to intentionally “access” a Federal Government computer without proper authority. All unauthorized use of Federal computers or information systems is a crime punishable by a fine of up to \$250,000 or a term of imprisonment of ten years. Accessing or providing someone with unauthorized access to a Government computer system is a serious crime regardless of the individual’s motives. Moreover, it is not a defense that a person did not know that the information was classified or that they were just “looking” around.

Tampering

Unlawful alteration of data on a computer system is also a crime. The person committing the act need not trespass on that particular system. For example, this situation often occurs when an employee

is authorized to access a computer system for a valid purpose but goes beyond the scope of that authorization and alters information by adding or deleting data.

Using a Government computer to operate a business or pyramid scheme

Using a Government computer to run a business or engage in a profit-making enterprise is a violation of Federal regulations and an abuse of Government resources. Such violations can be as simple as the employee who moonlights during work hours as a day trader or the employee who “borrows” web space on the Government-owned Local Area Network (LAN) to host his or her own personal real estate sales website. Likewise, solicitation of money, as part of a scheme whereby a recruit solicits money from others, who in turn solicit money from other recruits, is prohibited. These practices, known as pyramid schemes, can constitute fraud and could subject an employee to Federal wire fraud charges. Using a Government computer with intent to commit fraud is punishable by a fine of up to \$250,000 and five years in prison. In the case of a repeat offender, the maximum punishment increases to up to ten years.

Utilization of a computer in order to annoy, harass, or alarm another person

As stated earlier, oftentimes certain individuals misuse the anonymity of computers and particularly e-mail and the Internet, to infringe upon the privacy rights of others by annoying, harassing and, in the most serious cases, “cyber stalking” another person. Cyber stalking is similar to traditional stalking and occurs when an individual repeatedly harasses or threatens another, through e-mails and/or other electronic contact. It is often a serious problem in the workplace because unlike private e-mail users, Federal employees do not have the ability to readily change their e-mail addresses without significant difficulty and expense. Cyber stalking laws, prohibiting such harassing contact, are in effect in several states. At last count, 39 states, including New Jersey, have laws on their books expressly criminalizing this conduct. Federal employees should be aware of this type of activity and report it immediately. Most Government computers are monitored and often the offending conduct can be traced back to the user identification of the sender.

Viewing, access and possession of pornography

Federal employees must protect and conserve Government property and use it (or allow its use) only for authorized purposes. 5 C.F.R. § 2635.704(A). It is a violation of both Federal law and the Joint Ethics Regulation (DoDD 5500.7-R) to use a Government computer for unauthorized purposes such as accessing any type of pornography over the Internet. Pornography is generally broken down into the categories of adult and child pornography. While it is not against the law to possess or own adult pornography, it is a violation of Federal regulations to access it from a Government computer. There may be times when pop-up advertising to adult content websites appears on the screen during valid Internet surfing. However, should an employee inadvertently click on a link or view such a site, the employee should immediately notify his or her supervisor. Remember that most Government networks have software that will randomly check to see if these types of sites have been accessed. It is always best to be safe and let a supervisor know rather than take your chances that no one will find out.

Child pornography has been defined under Federal statute (18 U.S.C. § 2252) as a visual depiction of a minor (child younger than 18) engaged in sexually explicit conduct. The FBI actively

investigates matters involving the transmission, production and distribution of child pornography. Transmitting, or simply possessing, child pornography is illegal. The depiction of any child engaged in a sexual act, or an image that is obviously not “artistic” or serving any educational purpose, qualifies as pornography. This category includes images which are “morphed” or constructed of various body parts and do not represent living individuals. Computer telecommunications have become one of the most prevalent mediums used by pedophiles to share illegal photographic images of minors and to lure children into illicit sexual encounters. The Internet has dramatically increased sex offenders’ ability to access the population they seek to victimize. It is the responsibility and obligation of every Federal employee to report any information regarding instances of child pornography. It is a crime for anyone to possess even one child pornographic image whether electronic or otherwise. This is true even if the image is stored or viewed on a home computer. The penalty for possession of a single child pornography image includes a fine up to \$100,000 and imprisonment for a maximum of five years.

In addition to criminal penalties, civilian employees who misuse Government computers are subject to severe administrative penalties such as letters of reprimand, suspension and even termination. Military members may be punished under the Uniform Code of Military Justice (UCMJ) for failure to obey an order or regulation prohibiting the improper use of Government resources. Military members can face punishment ranging from reprimand or Article 15 all the way up to a General Court-Martial.

Internet-related crime, like other crimes, should be reported to appropriate law enforcement investigative authorities at the local, state, and Federal level. Several Federal law enforcement agencies investigate domestic Internet crime such as the FBI, United States Secret Service, United States Customs Service, United States Postal Inspection Service, and Bureau of Alcohol, Tobacco and Firearms (ATF). Each of these agencies has offices conveniently located in every state to which crimes may be reported. Contact information regarding these local offices may be found in local telephone directories. Employees who are aware of Federal computer crimes should report them to their immediate supervisors, the Army Criminal Investigation Division and local or Federal law enforcement agencies.

The Point of Contact for this subject in the CECOM Legal Office is CPT Michael Stephens (732) 532- 9813; DSN 992-9813.

KATHRYN T. H. SZYMANSKI
Chief Counsel