

## **Ask The Lawyer: Computer Misuse Can Compromise Security Clearance**

Q:

How bad is it for me to use my government computer for non-work matters?

A:

There is a type of computer program called a "Trojan horse." It usually comes to users as a benign message or link, but once opened it wreaks havoc on the computer system. You can view any misuse of your government computer, regardless of how innocent it seems, as a Trojan horse unleashed on your security clearance.

The System Authorization Access Request Navy (SAAR-N, OPNAV 5239/14) outlines the conditions of use, user responsibilities and prohibited uses relating to Navy information technology systems. SAAR-N prohibits users from, among other things, accessing commercial Web-based e-mail such as Yahoo! and introducing or using on any Navy IT equipment unauthorized hardware, firmware or software. Under SECNAV M-5510.30, a user's failure to adhere to a rule, procedure, guideline or regulation could threaten his or her security clearance.

SECNAV M-5510.30 provides a laundry list of ways the misuse of IT systems can cause security clearance problems. A few disqualifying activities include illegally accessing IT systems or doing so with without authorization; modifying, destroying, manipulating or denying access to certain information; and improperly introducing, removing or using hardware, software or media on or from an IT system.

Other misuses may also include conducting personal business on government time - stock trading, Internet purchases, and the like. Know your employer's rules about personal use of its computers. And avoid the obvious - porn sites and other prohibited sites, such as Wikileaks.

Simply clicking onto the link of an untrusted Web site while at work is enough to trigger a security clearance emergency due to the fact that this activity could expose Department of Defense systems to malware or viruses. Using an IT system to snoop on co-workers - or even what the government knows about you - would also call into question your trustworthiness and reliability.

Under SECNAV M-5510.30, Navy personnel could mitigate security concerns about IT use by showing that the misuse was minor, inadvertent, unintentional, happened a long time ago, or was an isolated incident. Navy personnel could also mitigate concerns by immediately reporting to a supervisor any unintentional or inadvertent misuse of their government computer. Navy personnel who have run into security clearance problems should immediately consult a national security law attorney, who could help them raise these mitigating factors during the adjudication process.

Mathew B. Tully is an Iraq War veteran and founding partner of the law firm Tully Rinckey PLLC . E-mail questions to [askthelawyer@fedattorney.com](mailto:askthelawyer@fedattorney.com)

. The information in this column is not intended as legal advice.