Don't Connect Personal USB Devices to Government Computers

But I'm just using a little power, what's the harm?

Anything that plugs into USB can not only draw power, but can also transfer data. USB provides both capabilities.

But I turned it off. So I'm ok right?

NO. USB supplies power; so, it's not necessary for the device to be on for data transfer to occur.

But it's not a thumb drive so what's the issue?

Even if it were as simple as a USB light or game controller, how do you know it doesn't have memory? All hard drives, mp3 players, phones, etc. definitely DO have storage and, in many cases, also include wireless capability which makes them a much greater vulnerability than a USB thumb drive. The introduction of these devices into US Government systems allows for the creation of an infection vector across classification boundaries.

But I don't transfer data back and forth. I would never load my data onto a work computer.

Within seconds of plugging in a USB cable, the computer and device start exchanging information. It's during this "handshake" period that a virus or malware can begin its work and infect any computer you plug into. This data transfer may introduce a cross-domain violation or the introduction of malicious data onto a US Government network.

But where would my portable device get a virus?

The Internet, Bluetooth vulnerabilities, infected media, other USB charging locations… the list is nearly endless. Not only is your device at risk of getting a virus, so are the government systems to which you are connecting.

Bottom Line

Personal devices can be charged on personal computers or with commercially available (and inexpensive) USB wall or car chargers. Plugging these devices into US Government systems creates vulnerabilities which lead to significant risks to our networks and, ultimately, our information.

Don't put your information at risk. Keep personal devices off of government systems!