InfoSec – August 2019

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

The ubiquitous nature of digital data and what to do about it

Wouldn't it be nice if digital data just vanished? Poof – it's gone.

Unfortunately, that is not the case. In fact, digital data seems to be somewhat related to cockroaches; it just won't go away no matter what we do or how hard we try. In fact, in many cases it seems to multiply without effort. For many, the <delete key> is our friend and in many situations using the delete key permanently removes the information unless the target of the delete key is a file.

For government contractors, the award of a contract may complicate the issue since FAR subpart 4.7 specifies requirements for Contractor Record Retention. As a result, instead of the contractor making a decision concerning when to dispose of different types of information, the contract and applicable contract clauses apply and must be consulted and followed.

Years ago, before computers and the arrival of digital data, we relied upon paper documents. These were portable to an extent but the hassle and cost of duplication was a type of braking mechanism to the creation of additional documents. It would be a rare case for someone to print a 100 page document for home use, print a second copy for work and just in case another copy was needed print a third or forth for the briefcase. So to a degree, having paper-based documents helped to limit reproduction and the spread of possibly sensitive information. Back then we also knew what information we had and where it was. Sure our inboxes were full and there were four drawer filing cabinets but to survive there needed to be a filing mechanism to organize information and assist with its retrieval.

Today, we live in a totally different environment; one that allows for email attachments, portable storage devices, digital download to both multiple computers and other mobile devices. Today, in a flash that 100 page document can be reproduced 3, 4, or more times. Instead of just one document to manage and control, there are multiple copies. Worse yet, this process can occur so quickly and with so many different documents that it is all but impossible to keep track of where each copy has been stored. To complicate matters, storage devices such as USB drives are relatively inexpensive and readily available. Instead of having just one or two devices to manage, even the average user has many, many more. In fact, USB devices are so popular that there are a variety of device storage systems available. After a year of two, many will have a collection of USB memory sticks and the faintest of ideas of what information is stored on each.

For companies that saw the value of technology and were early adopters of computers, their practices may have created additional copies of sensitive information on variety of storage mediums including floppy disks, CD's and even zip drives.

As a result, companies have to grapple with the some or all of the following –

1. Knowing/identifying what information they have
2. Knowing what device or devices it is stored on

3. Determining what information should/needs to be retained
4. Deciding how to consolidate identified information into a usable archive
5. How to destroy or permanently delete designated information
6. Finally, creating a digital data review and management policy

Moving forward, companies should consider developing a digital data storage policy and related procedures. These procedures should address controlling the creation of duplicate copies of sensitive (CUI, JCP, ITAR) or other information and its storage requirement, sharing/transmitting of information and how to properly destroy a device or delete specific information.

These procedures should address identifying which program each type of information is associated and required security measures.

For example in NIST 800-171 r1 required 3.1.19 specifies to "Encrypt CUI on mobile devices and mobile computing platforms." This reference also addresses the protection of CUI at rest and provides details and examples in the discussion –

"Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also employ other safeguards including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest." See NIST 800-171 - 3.13.16

Information related to the disposal of devices, the correct and permanent deletion of information and safeguarding of data can be found at the following federal resource - CISA - Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future.

Security Tip (ST18-005) Proper Disposal of Electronic Devices

See: https://www.us-cert.gov/ncas/tips/ST18-005

Security Tip (ST06-008) Safeguarding Your Data

See: https://www.us-cert.gov/ncas/tips/ST06-008