NASCIO Representing Chief Information Officers of the States

Issue Brief

February 2007

NASCIO Staff Contact: Stephanie Jamison; sjamison@amrms.com (859) 514-9148

The New and Improved DST: Are You Ready?

A little-noticed provision of the United States Energy Policy Act of 2005 is beginning to make headlines across the IT world as we approach the arrival of Daylight Saving Time (DST) – and it's going to come even sooner this year. The provision making waves among IT professionals stipulates that DST begin earlier in 2007 in order to preserve energy by prolonging daylight hours. Instead of the standard dates of the first Sunday in April and the last Sunday in October, the U.S. is set to "spring forward" our clocks on March 11, 2007 by one hour and "fall back" on November 4, providing an additional four weeks of DST.

Unfortunately, the manufacturers of IT systems, devices and software providers were not counseled before the measure was passed and the provision went virtually unnoticed until recently. Many applications and systems are already set to spring forward on April 1 and fall back on October 28, respectively. As a result, for the last three weeks in March, and for one week in October-November, applications and systems that are time and date-sensitive are going to be off by one hour – thereby giving the IT world a major headache.

There is however, a bright side – patches and fixes are available for most systems and can be found online. While this problem invokes memories of Y2K, the DST problem is on a smaller scale.

To accommodate the DST change, most IT systems must be patched. Otherwise, timestamps will be off, and some applications may fail to work. System administrators and IT employees must plan to apply these patches or fixes to any device having to do with dates and times. Real and anticipated consequences for failing to address this issue may mean more than a missed meeting or appointment – the entire system could be disrupted.

What State CIOs Need to Do

While many states have a remediation plan in place and are working to make certain corrective actions are completed before the new time change, there will no doubt be unintended consequences that cannot be anticipated. As a first step, it is important for the State CIOs to communicate the nature of this issue and the urgency of action to all state agencies. State CIOs should also review existing IT asset management data or take a thorough inventory of all assets including desktops, servers, databases, email messaging, smartphones, PDA's, and ***all other applications that have a* time-sensitive function or *maintain an internal clock.*** Many applications that do have an internal clock are run off a network, or are automatically set to change at certain dates. Suppliers of mobile devices, including wireless PDAs and smartphones, have already alerted users that the devices will not update their clocks for the new DST change and a software patch must be installed. For those devices or applications that are dependent on an hourly time stamp, manual intervention will likely be required.

Other systems, devices and applications that may be affected if no patches, fixes or adjustments are made include:

- employee time reporting systems
- electronic voting machines
- transaction receipts
- electronic submittals of payments, proposals, permits or license applications
- systems or applications with time-tracking logs
- electronic access control key card systems for facilities
- electronic PBXs, IVR and auto-attendant systems
- fax machines, copiers and multi-function products (MFP)
- switches, routers, NTP appliances
- mobile data capture devices
- electronic medical record notations
- intelligent transportation systems
- homegrown software applications

While a missed meeting or appointment may be inconvenient, an entire application or database entry that is operating on the wrong time may disrupt critical business processes and produce unwanted results if it goes unresolved.

Many software and application providers have already made patches and upgrades available online or offered remediation advice via their websites. State CIOs are encouraged to take a closer look at all applications and systems under their jurisdiction to ensure all appropriate fixes are applied to address the potential problems that may arise.