OCC Bulletin 2007-9| February 16, 2007

Daylight Savings Time Change: Risk Management Guidance

Purpose

This bulletin reminds national banks and their technology service providers of the upcoming change in the schedule for Daylight Savings Time. National banks may be exposed to a variety of risks if they do not prepare their systems to reflect this change.

Background

Daylight Savings Time (DST) in the United States will begin earlier and end later in 2007 than in years past. The Energy Policy Act of 2005, signed into law August 2005, moves the beginning of DST from the first Sunday in April to the second Sunday in March. DST will now end the first Sunday in November instead of the last Sunday in October.

Risk Management Considerations

The impact of the change in DST may not cause systems failures, but without remediation and preparation, banks could experience logging errors, monitoring difficulties, degraded system performance, or disruptions of some services. In addition, malfunctioning systems could result in compliance errors (e.g., incorrect ATM disclosures) and securities issues (e.g., malfunctioning security systems).

Bank management should understand the potential impact of the DST change on its hardware and software and plan for appropriate changes. Servers, mainframes, other important systems, and essential computer clock-dependent processes should be set to synchronize with the new time change. Management should review both date and time stamp processes and the many time-sensitive routines essential to information systems.

Major operating system vendors should have suitable patches available for the most current releases of their systems. Vendors of other systems and applications may also have patches available. If, however, no patch is currently available, bank management should confirm that its vendors will provide a suitable patch. Internally developed or customized systems may require custom patches or other special attention. Whether suitable patches are available or not, bank management should develop and implement strategies to appropriately mitigate risks associated with this time change.

Other systems may be affected as well; for example, those controlling heating, air conditioning, lights, alarms, telephone systems, and the opening of cash vault doors. If third parties provide time-sensitive services, management should ensure that the servicers are planning to make appropriate changes.

Management should consider the following actions to ensure readiness for the new start of DST:

To

Chief Executive Officers of all National Bank, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

- Review and verify modifications necessary for all important systems and essential processes, including servers, applications, and utility systems.
- Ensure that critical systems will synchronize and function properly by testing or other means.
- Determine which systems are connected to the USNO Master (Atomic) Clock through a network time protocol (NTP or NTPD) and whether they will synchronize with the master clock at the appropriate moment.
- Contact third-party service providers to ensure that the bank is protected.
- Determine whether the bank has systems that require a manual procedure to be performed and whether a follow-up plan is needed.
- Ensure that systems adjustments will not be duplicated when the historic change date occurs.
- Ensure that all employees throughout the bank are alerted to this change.

Several organizations, including the Financial Services Information Sharing and Analysis Center (FS-ISAC), recently issued alerts on this change. The OCC encourages bank management to consider participating in the FS-ISAC (www.fsisac.com) as part of an effort to detect and respond to intrusions and vulnerabilities.

For further information on or questions concerning the guidance, contact the Bank Information Technology Division at (202) 649-6340.

Mark L. O'Dell
Deputy Comptroller for Operational Risk