April 30, 2014

Information RE: Windows XP Support Ending

Extended support for Microsoft Windows XP Desktop Service Pack 3 (SP3) comes to an end on April 8, 2014, when Microsoft releases the last generally available security patches. Support for Microsoft Office 2003 also ends with the April 8 patch cycle. After April 8, Registered Entities will need to enter into a per-Cyber Asset custom support contract with Microsoft to continue to receive support for up to three additional years. Even then, not all vulnerabilities will be patched.

Cyber Assets running the Microsoft Windows XP Embedded SP3 operating system have until January 12, 2016, before support ends for that version of the operating system. And support for systems built on the Windows Embedded Standard 2009 operating system ends on January 8, 2019. The Windows Embedded operating system normally runs on appliances, and therefore, Registered Entities might not even realize the Windows Embedded operating system is in their operational technology environments.

The risk to Bulk Electric System reliability by continuing to rely upon Windows XP for critical operations applications after support ends is significant. Commonly, vulnerabilities in more recent versions of Windows, such as Windows 7, also exist in Windows XP. Attackers routinely reverse engineer security patches in a race to exploit identified vulnerabilities before system administrators can apply the patch. As patches will no longer be available for Windows XP, those vulnerabilities will become zero-day exploits. Additionally, third party application vendors, including anti-malware providers, are expected to cease support of Windows XP platforms, increasing the risk of exploitable vulnerabilities. The longer an entity continues to run Windows XP, the more at-risk those vulnerable systems become.

Registered Entities still running Windows XP Desktop or Embedded should already be well on the way to migrating to a supported operating system. If an Entity has not started a migration project, it needs to start immediately. The first step is to contact the software providers for assistance. Entities should work with the vendor to develop a migration plan that includes thorough testing, and be prepared to migrate to a different vendor's solution if necessary.

In the interim, there are mitigating measures that should be evaluated and implemented as applicable. While not eliminating the risk entirely, these mitigations will reduce the overall risk by reducing the attack surface. Consider the following:

- Review enabled ports and services on the Cyber Asset. Disable any service that is not required for operations, whether or not it raises a Listening port.

- Review firewall rules. Ensure that all unnecessary or discretionary access is removed. If at all possible, deny all access from outside the security perimeter to the Cyber Assets running Windows XP. That includes denying all remote access from the corporate or external networks for maintenance and support purposes. Additionally, define firewall rules that block all unnecessary outbound traffic from the vulnerable systems. Log all access failures and review the logs at least daily if not in real time, investigating any blocked access log messages.

- Ensure anti-virus and other anti-malware solutions are running on any Cyber Assets running Windows XP and that the signature files are up to date. Signature files should be updated at least daily.

- Do not allow any non-essential use of the vulnerable Cyber Asset supporting critical operations. This is especially important for Control Center operator consoles. Migrate non-essential tasks to a different workstation that resides outside of the secure critical operations networks.

- Do not allow the use of removable media (e.g., CD/DVD, flash drives, and external hard drives) whenever possible on any secure critical operations network that contains a Cyber Asset running Windows XP. If the use of removable media cannot be avoided, fully scan all such media before introducing the removable media into the secure network environment. Use a dedicated, single purpose, fully patched workstation for media scanning that is connected to a protected network outside of the secure critical operations network and running the latest anti-virus software and up-to-date signature files. Do not perform any other function on the scanning workstation.

- Perform frequent system backups and verify all information required to restore a failed or compromised Cyber Asset has been retained by performing a test restoration on a spare Cyber Asset. Ensure the backup information includes documentation of all configuration and hardening parameters.

- Consider implementing a white-listing anti-malware solution on any Cyber Asset running Windows XP. White-listing solutions prevent software from running that has not been explicitly approved and can be a very effective way to prevent malware from compromising a protected Cyber Asset.

Please contact Kevin Perry (501-614-3251) or Tyler Morgan (501-614-3521) with questions.