As you are probably aware, Microsoft has indicated that it will discontinue support for the Windows XP operating system on April 8, 2014. After this date, Microsoft will no longer provide free security updates or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safe. PCs running Windows XP after April 8, 2014, should not be considered to be protected, and additionally, will not be considered to be compliant with the FBI’s CJIS Security Policy. If you are unable to remediate any XP based PCs that connect to DPS by April 8, DPS suggests that you employ the following compensatory measures.

(The following information has been derived from the United States Computer Emergency Readiness Team. For additional information, please reference [http://www.us-cert.gov/ncas/alerts/TA14-069A-0](http://www.us-cert.gov/ncas/alerts/TA14-069A-0).)

**General Compensatory Measures for Windows XP (XP) Systems**

- For those that are unsure what OS they may be running, Microsoft provides an, “Am I running XP?” site ([http://goo.gl/PFbCpg](http://goo.gl/PFbCpg)). Upon visiting the site, a large message displays to indicate whether the end user is or is not running XP.

- Microsoft is encouraging users to upgrade to Windows 7/8, but reminding them that older computers may not meet system requirements. In these cases, Microsoft suggests upgrading to a new computer. For those looking to upgrade to a new computer, Microsoft is also offering Laplink PC mover Express to offer free assistance in moving data from an old XP computer to a new Windows PC.

- Microsoft will continue to support the Microsoft Security Essentials product through July 14, 2015. For enterprise customers this includes System Center Endpoint Protection, Forefront Client Security, Forefront Endpoint Protection and Windows Intune.

- Microsoft will also offer *Custom Support* Agreements as a last resort for those that do not expect to complete migration to a new OS in time. Use of this support requires additional funds to be expended on a per computer basis.

- Of 26 antivirus vendors, AV-TEST ([http://goo.gl/PCLZNL](http://goo.gl/PCLZNL)) provides a list of 22 that will continue to push updates to their suites on XP, which will aid in protection after Microsoft ends support.

**Supplementing Security: Custom Built Applications**

Many organizations may find upgrading to a different OS challenging as some have chosen to build custom applications on XP. Of these custom-built applications, some are still in use for mission-critical projects today and will not easily transfer to Windows 7/8. The following options, or a combination of them, may be useful for organizations running custom XP applications:

1. Hire the person who built the application to rewrite the application and make it compatible with other operating systems.

2. Shim the app, or “trick” the application into thinking it is running in an XP environment. This option is unstable, risky, and it may not work.

3. Virtualize the application so that it will work in a different operating system.

4. Continue to use the XP computer on an interim basis; however, lock-down administrative rights and do not let anything new be installed on it (virtual applications would be a good route here, as they do not require installations to run). This is a worst-case scenario and would only be a temporary option.
Supplementing Security: Individual End Users

The following recommendations are for individual end users using XP computers until they are migrated to Windows 7/8:

- Air-gap or isolate on separate networks XP computers in order to protect updated machines from being attacked by compromised XP computers.

- Install the final XP update so computers start their unsupported lives protected from the latest known vulnerabilities.

- Install an alternative browser (i.e. Firefox or Chrome) and make it the default. XP comes with Internet Explorer but it only supports up to IE 9, making the security features of IE 10 and 11 unavailable.

- Fully patch Microsoft Office to reduce the chances of it being used to compromise the XP computer.

- Uninstall unused third-party software. The older it is, the more likely it is to be vulnerable.

- Consider disabling or uninstalling browser plugins for third-party software, and set the browser to ask what to do with PDFs, etc., rather than opening them by default.

- Install up-to-date firewalls and anti-virus software.

- Keep the computer on a trusted network behind a NAT router, which acts as a hardware firewall.

- Upgrade to Windows 7/8 as soon as possible.

Mike Lesko
Deputy Assistant Director
Law Enforcement Support Division
Texas Department of Public Safety