IMPACTS TO CISCO CUSTOMERS DUE TO END OF SUPPORT FOR OLDER VERSIONS OF INTERNET EXPLORER *and* INDUSTRY END OF LIFE FOR SHA-1 SECURITY CERTIFICATES

January 12, 2016

1. INTERNET EXPLORER

Background: Microsoft recently announced that beginning January 12, 2016, only the latest version of Internet Explorer (currently Internet Explorer 11) will receive technical support and security updates from Microsoft for supported Windows operating systems (which currently include Windows 7, Windows 8.1, and Windows 10). After January 12, 2016, Microsoft will no longer provide security updates or technical support for older versions of Internet Explorer, leaving those versions more susceptible to malware and other security attacks. Details can be found at: https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support .

Impacts to Customers with Cisco Contact Center Products

- All Cisco Customer Care 10.5, 10.6, and 11.0 products currently support IE 11, so any customer using these versions of Cisco CC software should upgrade to IE11 in order to run a browser supported by Microsoft.
- Pre-10.5 versions of some Cisco Customer Care products do not support IE 11. Cisco plans to *retroactively support* IE 11 with Contact Center 10.0 products. For some products, this is a testing effort only. For other products, patches may be issued to provide fixes to issues that may be discovered during IE 11 testing. Official support of IE 11 on all Cisco Customer Care 10.0 products is expected within the next few months. When available, updated product software can be downloaded from: https://software.cisco.com/download/navigator.html?mdfid=285971052 (Cisco.com login required)
- Cisco does *not* plan to support IE 11 on Customer Care product versions earlier than 10.0.

2. SHA-1 CERTIFICATES

Background: As of January 2016, certificate authorities will no longer generate SHA-1 certificates. After January 2017, internet browsers will no longer accept SHA-1 certificates. SHA-2 certificates must be supported for browser products to continue working after January 2017. Details can be found at:

- http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html
- http://www.zdnet.com/article/google-accelerates-end-of-sha-1-support-certificate-authorities-nervous/
- http://www.symantec.com/connect/blogs/how-manage-sha-1-deprecation-ssl-encryption

Impacts to Customers with Cisco Contact Center Products
The impact and mitigation for Cisco Customer Care products/components is different depending on the version of the product and the underlying operating system.

11.0 Components:

- **VOS Products (e.g., Finesse, CUIC, Live Data**) – SHA-2 certificates work correctly but Cisco is updating our documentation to make this clear. Also, the default certificates that ship with the products are SHA-1, so Cisco will provide instructions on how to regenerate the certificates to make them SHA-2 compliant.
- **Windows (ICM, CVP)** – SHA-2 works for 3rd party certificates, but Cisco will provide a patch to generate SHA-2 instead of SHA-1 certificates. When available, updated product software can be downloaded from: https://software.cisco.com/download/navigator.html?mdfid=285971052 (Cisco.com login required)

10.6, 10.5, and 10.0 Components:

- **VOS Products** – Cisco will issue a patch so that SHA-2 certificates can work correctly.
- **Windows –** Same as v11. SHA-2 works, but a patch is required to make the certificates SHA-2 compliant.