Notes to Release Notes Authors

IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPG-QT**
Release Version	**2.0b**
Release Date	**04/18/2018**
Previous Version	**2.0a**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated CPU microcode to address 'Spectre' variant 2 (CVE 2017-5715) security issue.** **2. Enabled IERR crash dump function.** **3. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.** **4. Updated 5.12_PurleyCrb_0ACFD085Beta for Purley Skylake platform PLR 4, BKC WW02.** **5. Displayed setup item "ACS Control" to Enable/Disable PCIe Access Control Services Extended Capability, with Enabled as default.** **6. Changed BIOS revision to 2.0b.** **7. Added support for M/B 1.10A with 32MB BIOS chip.**

New features	**1. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.** **2. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.**
Fixes	**1. Fixed problem of yellow marked device appearing in Windows device manager after S3 resumes.** **2. Corrected the "Save Changes" setup option string in "Save & Exit" menu.** **3. Disabled SNC once NVDIMM is present in system.** **4. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.** **5. Fixed problem of TPM 2.0 PS NV Index not being write-protected even if customized provisioning table indicates that it must be write-protected when using "SMC OOB TPM Provisioning via IPMI feature".** **6. Fixed problem of system rebooting endlessly when equipping dTPM module.** **7. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.** **8. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.** **9. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.** **10. Disabled CPU2 IIO PCIe root port ACPI hot plug function.** **11. Fixed issue with IPMI force boot.** **12. Fixed issue of all commands requesting to be persistent.** **13. Fixed malfunction of "SMBIOS Preservation" Disabled.** **14. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.** **15. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.** **16. Fixed inability to set memory policy.**

	17. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled. **18. Fixed failure of BIOS ECO ATT test case 306.** **19. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.** **20. Fixed failure of SATA HSIO register setting test.**