IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPH-I/T/TQ**
Release Version	**2.1**
Release Date	**6/15/2018**
Previous Version	**2.0b**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.** **2. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.** **3. Updated 5.12_PurleyCrb_0ACFD087Beta for Purley Skylake platform PLR6, BKC 2018 WW14.** **4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.4.0.1039.** **5. Corrected BIOS/ME downgrade check for SPS 4.0.4.340.** **6. Added SMC_BUS_MASTER_EN token for enabling SMC Bus Master or AMI DMA AMI BME DMA Mitigation in setup.** **7. Updated Giga LAN EFI driver 8.3.0.4 (IBA 23.1).** **8. Added support for UEFI mode PXE boot of F12 hot key Net boot.** **9. Added support for RFC3021.** **10. Corrected default setting for Enable SmcBusMasterEn setup item.** **11. Checked PCH SKU for QAT enabled board.**

New features	N/A
Fixes	1. Fixed problem of system hanging when installing Linux OS after COM1 & COM2 IO/IRQ exchange. 2. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS. 3. Fixed problem of DMI being lost if DMI is changed and then UpdateBios is run. 4. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller. 5. Fixed failure of WDT function.

2.0b (2/27/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.
3. Updated Purley RC 151.R03.
4. Updated BIOS ACM 1.3.5 and SINIT ACM 1.3.3.
5. Changed PCH uplink CTLE/VGA/TSM SI setting to [4,10,32].
6. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.
7. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.
8. Disabled CPU2 IIO PCIe root port ACPI hot plug function.
9. Fixed issue with IPMI force boot.
10. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.
11. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.
12. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.
13. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.
14. Fixed problem of the system not logging memory errors upon injection without rebooting.
15. Fixed inability of BIOS to boot into OS with Intel P3608 PCIe NVMe drive installed.