IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPT-L**
Release Version	**3.3**
Release Date	**02/21/2020**
Previous Version	**3.2**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated AMI label 5.14_PurleyCrb_0ACLA050 beta for IPU2020.1 PV.** **2. Updated BIOS ACM 1.7.40 and SINIT ACM 1.7.48 PW.** **3. Enabled saving memory CE location into PPR variable at runtime even if memory correctable error reporting is disabled.** **4. Added sighting CLX28 workaround and downgraded patrol scrub UC to CE.** **5. Updated Skylake-SP/Cascade Lake-SP CPU microcode from Intel-Restricted-2020-1-IPU limit beta.** **6. Added SMC HDD Security feature.** **7. Updated SPS_E5_04.01.04.381 from IPU 2020.1 PV.** **8. Added setup item "HDDword prompt Control" to control "Hard-Driveword Check" to enable/disable HDDword prompt window during POST.**

	9. Updated setup menu to remove our own tRFC optimization item, add Intel "tRFC Optimization for 16Gb Based DIMM" and "Panic and High Watermark" items, and add "Balanced Profile" option for "DCPMM Performance Setting".
New features	
Fixes	**1. Fixed mismatch of Secure Boot Mode value.** **2. Fixed malfunction of onboard SAS option ROM control.** **3. Fixed Intel Self test 7 v111 SPI/DCh BIOS_CNTL to set BIOS Control Register BIT[9] to 1.** **4. Fixed inability to log UPI correctable error.** **5. Fixed problem of system hanging at POST code 0x92 with Apacer M.2 SSD.** **6. Removed requirement to use Admin password for erasing TCG device.** **7. Fixed problem of two CentOS boot items occurring in boot order if CentOS is installed in RAID 1 system.**

Release Notes from Previous Release(s)

3.2 (10/17/2019)

1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated Intel BKCWW16 2019 PV PLR1.
3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
4. Updated EIP467272 for AMI SA50069, SA50070.
5. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. Enhanced F12 hot key PXE boot feature.
9. Updated AMI label 5.14_PurleyCrb_0ACLA049_BETA for BKC WW36 IPU 2019.2 and AMI security update SA50072.
10. Updated SINIT/BIOS ACM from BKC WW36 IPU 2019.2 to address CVE-2019-0151 and CVE-2019-0152.
11. Updated SPS_E5_04.01.04.339.0 from BKC WW36 IPU 2019.2 to address PSIRT-TA-201905-011.
12. Updated Cascade Lake-SP CPU microcode and Skylake-SP microcode.
13. Displayed Setup item "ARI Support".
14. Added setup item to control 16Gb based Single Die Package DIMM tRFC optimization.
15. Updated Secure Boot Key to fix the error message of PK key.

16. Patched inability of system to boot via onboard LAN2 after IPMI forces PXE boot when there is an OS behind LSI-3108 RAID card.
17. Added back erase NVDIMM routine.
18. Updated VBIOS and VGA EFI Driver to 1.10.
19. Enhanced F12 hot key PXE boot feature.
20. Updated the behavior for the feature that updates SMBIOS Type 1 and 3 with FRU0.
21. Added support for SMC HttpBoot.
22. Disabled ADDDC/SDDC and set PPR as hPPR.
23. Added Enhanced PPR function and set disabled as default.
24. Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.
25. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
26. Set ADDDC to enabled by default.
27. Removed PXE option for "OnBoard LanX Option ROM" when "Boot mode select" is UEFI.
28. Corrected display of the IPMI AUX revision.
29. Changed OOB download and Upload Bios Configuration sequence.
30. Fixed problem of two OS (Redhat & Ubuntu) boot devices appearing in boot order.
31. Fixed failure of OPROM control item if CSM is disabled.

3.1 (5/21/2019)

1. Updated Skylake-SP/Cascade Lake-SP CPU microcode.
2. Updated Intel BKCWW16 2019 PV PLR1.
3. Updated SPS_E5_04.01.04.296.0 from BKC WW16 2019.
4. Updated EIP467272 for AMI SA50069, SA50070.
5. Set SDDC Plus One or SDDC to disabled by default.
6. Updated SATA/sSATA RAID OPROM/EFI driver to VROC PreOS v6.1.0.1017.
7. Set Leaky Bucket that can decrease one memory correctable error count within 2.15 minutes with threshold 512.
8. Enhanced F12 hot key PXE boot feature.
9. Improved help messages of Intel VMD.
10. Fixed problem of system halting or rebooting at POST code 0xB2 or 0x92 when total GPT partition number is more than 256 and RSD is enabled.
11. Fixed inability to change IPv6 address or IPv6 Router1 IP address.
12. Set ADDDC to enabled by default.

3.0c (3/27/2019)
1. Added support for Purley Refresh platform.
2. Enhanced BIOS setup menu to switch the boot mode value and Option ROM's values when CSM support is disabled and applied this to enabled secure boot mode case.
3. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes.
4. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Added support for RFC4122 UUID format feature to set RFC4122 encoding from build time produced by IPMICFG 1.29 tool or newer.
7. Updated CPU microcode SRV_P_262 for Skylake-SP H0/M0/U0 CPUs.
8. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.
9. Added 2933 to memory POR.
10. Added support for Linux built-in utility efibootmgr.

11. Updated valid range of IPMI setup item VLAN ID to 1-4094.
12. Added driver health warning message.
13. Set NVDIMM ADR timeout to 600µs.
14. Prevented inability to flash BIOS by AFU or SUM in-band when JPME2 CMOS value is not excepted.
15. Added a help/reminder message to appear when user incorrectly selects "EFI" for "Onboard Video Option ROM" but boots to legacy.
16. Updated to SPS 4.1.02.174 or above for INTEL-SA-00185 Security Advisory and to RC 549.D13 or above for INTEL-SA-00192 Security Advisory.
17. Added support for Cascade Lake CPU.
18. Updated to SPS 4.0.04.381 or above for INTEL-SA-00213 Security Advisory.
19. Applied workaround for inability of SUM to get full setting of IODC setup item.
20. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
21. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail").
22. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard.
23. Patched problem of system hanging at 0x94 when plugging in Nvidia Tesla T4 card.
24. Fixed incorrect display of the TDP of Intel Speed Select table.

2.2 (12/6/2018)
1. First Release