IPMI Firmware / BIOS Release Notes Form

Product Name	X11DPT-B
Release Version	2.0
Release Date	11/30/2017
Previous Version	1.0a
Update Category	Critical
Dependencies	None
Important Notes	N/A
Enhancements	1. Updated 5.12_PurleyCrb_0ACFD084 for Purley Skylake platform PLR 3.1. 2. Updated CPU microcode SRV_P_214 for Skylake-EP H0/M0/U0 stepping CPUs. 3. Updated SPS 4.00.04.294 PLR 3.1 PV version. 4. Updated BIOS ACM 1.3.4. 5. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1052. 6. Added support for AOC-SLG3-2M2 card on CPU1 SLOT1. 7. Updated ShellBinPkg_08 for CapsLock/NumLock malfunction. 8. Exported "IMC Interleaving" item for performance tuning. 9. Displayed "PCIe PLL SSC" setup item for clock spectrum function. 10. Updated help string for tCCD relax setup option. 11. Set to show recovery error message when no BIOS image is in USB pen drive.

	12. Added the "PEI--IPMI Initialization" Post-Help message.
	13. Enabled display of EarlyVideo message by onboard video when VGA Priority is set to Offboard.
	14. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.
	15. Allowed runtime memory UCE mapout message to be displayed one time during BIOS POST.
	16. Set to avoid TCG protocol "PassThroughToTpm" failure under EFI shell when user enables "TXT Support" with disabled "TPM state" in TPM 1.2 BIOS setup menu.
	17. Enabled RSD/JBOF support.
	18. Hid "IPMI" and "Secure Boot" forms for SUM.
	19. Removed PCI PERR/SERR Support item and enabled reporting PCIe error by default.
New features	1. Set flashing BIOS/ME to be skipped when trying to downgrade the SPS ME firmware from 4.0.4.288 to previous version.
	2. Set display of setup option for always turbo mode function as default.
	3. Implemented SMC Recovery Flash Boot Block Feature.
	4. Removed support for Ctrl+home triggering recovery.
	5. Added BUS number out of resource auto assignment solution from AMI for RSD/JBOF support.
Fixes	1. Fixed inability of Intel P3100 M.2 to boot to OS.
	2. Fixed problem of BMC PCIe root port being forced to Gen1.
	3. Fixed failure of setup item "Install Windows 7 USB support".
	4. Fixed malfunction with SMCSataFrozen item.
	5. Updated BMC LAN configuration for saving settings of BIOS setup menu.
	6. Removed setup item "IPV6 Support" load default function.
	7. Fixed inability to enter setup menu when pressing "DEL" key if there is no boot device.

	8. Fixed problem of changes to CPU core Enable/Disable in setup menu sometimes not taking effect on Windows OS.
	9. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.
	10. Fixed failure of Password Preservation Test due to password not being preserved.
	11. Fixed problem of the Last-runtime-memory-UCE causing system to hang at POST 0x79.
	12. Fixed the Runtime UCE memory causing DIMM mapout to not be shown on screen.
	13. Fixed problem of the string of "Error DIMM information" on screen being corrupted when equipping failed DIMM.
	14. Fixed problem of TPM 2.0 BIOS-Based Provisioning table not setting PW flag to PS LCP Data for production platform.
	15. Fixed inability of the system to enter TXT Environment when using TPM 1.2 on production platform.
	16. Fixed problem of TPM 1.2 PS index not being Write-Protected so that the content of TPM 1.2 PS index still can be modified after TPM 1.2 is nvLocked.
	17. Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.
	18. Fixed problem of system hanging when using AFUWIN/AFULNX to flash BIOS under OS.
	19. Fixed problem of DMI clearing when running SUM LoadDefaultBiosCfg or clearing CMOS with JBT1.