IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPG-TF**
Release Version	**1.0a**
Release Date	**11/17/2017**
Previous Version	**1.0**
Update Category	**Critical**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Added the "PEI--IPMI Initialization" Post-Help message.** **2. 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.** **3. Updated help string for tCCD relax setup option.** **4. Added setup item for Samsung tRWSR workaround.** **5. Corrected help string of setup item "Enforce POR".** **6. Updated new MRC error log definition.** **7. Allowed runtime memory UCE mapout message to be displayed one time during BIOS POST.** **8. Updated CPU microcode SRV_P_209 for Skylake-EP H0 stepping CPUs.** **9. Increased SataRaidOromDelay & SataRaidOromDelay to 6 seconds.** **10. Updated ShellBinPkg_08 for CapsLock/NumLock malfunction.**

	11. Reduced the boot time caused by IPv4/IPv6 polling. **12. Added "SMBIOS Preservation" Enabled/Disabled item for flash recovery.** **13. Added support for AOC-SLG3-8E2P and AOC-SGL3-4E2P.** **14. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.3.0.1041.** **15. Updated SPS 4.00.04.288 PLR version for security vulnerabilities.** **16. Updated BIOS ACM 1.3.4.** **17. Updated CPU microcode SRV_P_211 for Skylake-EP H0 stepping CPUs.** **18. Updated 5.12_PurleyCrb_0ACFD083_BETA for Purley Skylake Platform BKC WW39.** **19. Moved Run Sure item to Memory RAS Configuration setup page.** **20. Updated ME XML VSCC table to support 32MB SPI chip 25L25635E/MX25L25635F/MX25L25673G.** **21. Masked off PCIe correctable and non-fatal errors.** **22. Added support for AOC-SLG3-2M2 card.** **23. Hid "Enable ADDDC Error Injection" setup item.** **24. Set PCIe correctable error to not log and legacy PCI PERR or SERR error to still log.** **25. Removed PCI PERR/SERR Support item and enabled reporting PCIe error by default.** **26. Set eSPI clock to 24MHz and added support for Quad IO mode.**
New features	**1. Displayed setup item "Core Disable Bitmap(Hex)" in BIOS CPU Configuration page.** **2. Added Run Sure setup item.** **3. Set BIOS/ME flashing to be skipped when trying to downgrade the SPS ME firmware from 4.0.4.288 to previous version.**
Fixes	**1. Corrected SMBIOS Type 9/40 information for CPU1 PCIe slot.** **2. Fixed failure of Password Preservation Test due to password not being preserved.**

	3. Fixed problem of the string of "Error DIMM information" on screen being corrupted when equipping failed DIMM. **4. Updated BMC LAN configuration for saving settings of BIOS setup menu.** **5. Fixed inability of Intel P3100 M.2 to boot to OS case.** **6. Fixed inability to enter setup menu when pressing "DEL" key if there is no boot device.** **7. Fixed malfunction with SMCSataFrozen item.** **8. Fixed failure of SMBIOS Type 20 to fill Interleave Position and Interleaved Data Depth correctly.** **9. Fixed problem of system hanging when set to NVMe VMD mode for CPU PCIe Root Port.** **10. Fixed BMC PCIe root port being forced to Gen1.** **11. Fixed problem of the Runtime Uncorrectable Memory error injection causing system to enter into endless reboot at POST code 0xEE.** **12. Fixed the Endless reboot caused by Last-time-uncorrected-memory error.** **13. Fixed inability of Intel RC Setup strings to appear in SUM BiosCfg file when booting to OS directly.** **14. Fixed problem of serial console output showing SMC logo when EarlyVideo logo item is disabled.** **15. Fixed problem of the Last-runtime-memory-UCE causing system to hang at POST 0x79.** **16. Fixed problem of CMOS write sometimes being unstable.** **17. Fixed problem of the Last UCE report (mapout) DIMM sometimes not matching real UCE DIMM location.** **18. Corrected Hynix DIMM info to "SK Hynix".** **19. Fixed inability to report PCI-e error event in PCH slot.**

	20. Fixed problem of IPMI SEL logging "Memory training failure." and "No memory DIMM detected, install memory DIMMs." twice per reboot. **21. 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.** **22. Fixed problem of system hanging when using AFUWIN/AFULNX to flash BIOS under OS.**