IPMI Firmware / BIOS Release Notes Form

Product Name	**X11SPG-TF**
Release Version	**2.0b**
Release Date	**04/12/2018**
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. Added setup item "SmcBusMasterEn" for enabling Parent bridge of the devices in the gSmcPciForceEnableBusMasterList.** **3. Updated "Power Technology" callback solution.** **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. Enabled IERR crash dump function.** **7. Changed maximum speed in SMBIOS type 4 to 4500Mhz.** **8. Added one event log to record that the event log is full.** **9. Added support for VMD settings to be preserved after flashing, with enabled as default.**

New features	**1. Changed RC default setting to upgrade POST Memory correctable error to uncorrectable error and map out the channel.** **2. Implemented SMC OOB TPM Provisioning via IPMI Feature for customized provisioning table.**
Fixes	**1. Fixed issue with IPMI force boot.** **2. Fixed issue of all commands requesting to be persistent.** **3. Fixed problem of incorrect memory access on OOB causing system to hang.** **4. Fixed malfunction of "SMBIOS Preservation" Disabled.** **5. Fixed problem of SMC skipping first boot option in UEFI mode when retrying boot.** **6. Fixed problem of the endpoint PCIe device having error bits in PCI Status or Device Status register.** **7. Fixed inability to set memory policy.** **8. Fixed inability to reset the system under DOS by pressing "Ctrl-Alt-Del" on USB keyboard when "Port 60/64 Emulation" is disabled.** **9. Fixed problem of some platforms hanging up at POST code 0xB2 when equipping dTPM module.** **10. Fixed problem of DMI being cleared when running SUM LoadDefaultBiosCfg.** **11. 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".** **12. Fixed problem of system hanging during BIOS flashing if Watch Dog function is enabled.** **13. Corrected the "Save Changes" setup option string in "Save & Exit" menu.** **14. Fixed problem of changing CPU Core Enable/Disable in setup menu sometimes not taking effect on Windows OS.** **15. Fixed problem of system generating abnormal strings under DOS after triggering SERR or PERR error event in PCH slot.**

	16. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.