IPMI Firmware / BIOS Release Notes Form

Product Name	**X11DPFR-S(N)**
Release Version	**3.0c SPS: 4.1.04.256**
Release Date	**3/28/2019**
Previous Version	**3.0a**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated Intel BKCWW10 2019 PV MR3.** **2. Updated SPS_E5_04.01.04.256.0 from BKC WW08 2019.** **3. Updated Skylake-SP/Cascade Lake-SP CPU microcode from SRV_P_272.** **4. Updated standard NVDIMM ADR time.** **5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.** **6. Disabled unused SPS ME "CUPS IIO" and "Volumetric Airflow" sensor.** **7. Added support for Linux built-in utility efibootmgr.** **8. Updated valid range of IPMI setup item VLAN ID to 1-4094.** **9. Added driver health warning message.** **10. 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.**

	11. Enhanced BIOS setup menu to auto-switch the Option ROM's value and hide the unexpected value when boot mode changes. 12. 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.
New features	N/A
Fixes	1. Fixed failure of CPU PBF (Prioritized Base Frequency). 2. Added workaround for failure of BIOS flash with 156 bytes PubKey (Error: "Secure Flash Rom Verify Fail"). 3. Modified UEFI network description to IPv4/IPv6 to follow Industry Standard. 4. Applied workaround for inability of SUM to get full setting of IODC setup item. 5. Fixed failure to boot into VMware OS when set to Maximum Performance even if Monitor/MWAIT is enabled. 6. Temporarily fixed error for SKX (CLX) 4114 CPU memory training with Micron (18ASF2G72PDZ-2G6E1) RDIMM.

3.0a (1/12/2019)

1. Added support for Purley Refresh platform.
2. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v6.0.0.1024.
3. Updated Giga LAN legacy PXE/legacy iSCSI OPROM driver to IBA 23.2 and uEFI driver to IBA 23.5.
4. Set BMC MAC address to UUID for system without onboard LAN1 or with onboard LAN1 disabled.
5. Set PCIe correctable and uncorrectable (non-fatal) error report to disabled by default.
6. Set RFC4122 encoding to only be enabled for build time produced by IPMI 1.29 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 support for Linux built-in utility efibootmgr.
10. Updated valid range of IPMI setup item VLAN ID to 1-4094.
11. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.

2.1a (10/23/2018)

1. Added support for Monitor Mwait feature.
2. Fixed inability of VMD status to load default if loading default by AFU.
3. Updated SATA RAID OPROM/EFI driver to RSTe PreOS v5.5.0.1028.
4. Updated SPS 4.0.4.393 to correct problems of unexpected SPS response to HECI Host Config cmd with PStatesRatio Missing when HWPM is enabled as OOB or Native without legacy, and of duplicated EID being assigned on MCTP endpoint after sending MCTP force discovery IPMI command.
5. Updated SATA RX DWORD20 Ports 0, 1, 2, 4, 5, and 6 to ~2.4dB and ports 3 and 7 to ~1.6dB.
6. Synchronized setup menu string and SMBIOS type9 slot description.
7. Fixed problem of system resetting while flashing BIOS under OS if Watch Dog function is enabled.
8. Fixed malfunction of BIOS/ME downgrade check when running flash package (SWJPME2) a second time.
9. Fixed problem of BIOS always retrying boot when Re-Try Boot is Disabled.
10. Fixed malfunction of support for LEGACY to EFI.
11. Fixed issue with IPMI firmware capability.
12. Fixed failure of turbo in new Linux kernel.
13. Fixed inability to set memory policy.
14. Fixed problem of setup item "Quiet Boot" staying enabled after flashing BIOS with "Quiet Boot" disabled.
15. Fixed problem of system hanging after downgrading BIOS from 2.1a to 2.1.

2.1 (7/13/2018)

1. Updated CPU microcode to address 'Spectre' derivatives (CVE-2018-3639 & CVE-2018-3640) security issue.
2. Updated 5.12_PurleyCrb_0ACFD088Beta for Purley Skylake platform PLR7, BKC 2018 WW20.
3. Corrected default setting for Enable SmcBusMasterEn setup item.
4. Added hidden item "Early Console Logo".
5. Added support for RFC3021.
6. Updated BIOS ACM 1.3.7 and SINIT ACM 1.3.4.
7. Fixed problem of Ctrl + Alt + Del causing system to hang after flashing BIOS.
8. Fixed problem of SUM GetSataInfo showing incorrect "Configuration Type" when setting "Configure sSATA as" to "AHCI" or "RAID" on sSATA controller.
9. Fixed problem of the NVMe drivers not showing temperature and ejecting when only one CPU is

installed and AOC-SLG3-2E4T is on CPU1 RP1.
10. Fixed problem of DMI being cleared when running SUM UpdateBios.
11. Displayed setup items for JEDEC NVDIMM.

2.0b (2/24/2018)

1. Implemented enhancement to address 'Spectre' variant 2 (CVE 2017-5715) security patch issue.
2. Changed maximum speed in SMBIOS type 4 to 4500Mhz.
3. Added support for AOC-SLG3-2E4T only for two NVMe drives.
4. Added support for System Firmware Progress System Firmware Progress feature.
5. Added support for BPN-SAS3-F424-A6N4 panel for six NVMe drives.
6. Fixed inability of some CPUs to display correct microcode revision under BIOS setup menu.