BIOS Release Notes Form

Product Name	**X12DPD-A6M25**
Release Version	**1.9 SPS: 4.4.4.603**
Build Date	**01/11/2024**
Previous Version	**1.5**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated source base to 5.22_WhitleyCrb_0ACMS_ICX_077 (2024.1 IPU-PV).** **2. Updated Dx/Mx PC microcode Intel-Restricted-2024-1-IPU-20231009_20241IPU for IPU2024.1.** **3. Updated Intel Server Platform Services for Whitley Server Platforms IPU2024.1 4.4.4.603.** **4. Fixed how the ATT Test case "Check BBS test" failed when using Windows OS for test problem.** **5. Added mapping language for SGX related items.** **a. Mapping language of item Software Guard Extensions Epoch 0 is CSPWL070.** **b. Mapping language of item Software Guard Extensions Epoch 1 is CSPWL071.** **c. Mapping language of item SGXLEPUBKEYHASHx Write Enable is CSPWL072.** **d. Mapping language of item SGXLEPUBKEYHASH0 is CSPWL073.** **e. Mapping language of item SGXLEPUBKEYHASH1 is CSPWL074.** **f. Mapping language of item SGXLEPUBKEYHASH2 is CSPWL075.** **g. Mapping language of item SGXLEPUBKEYHASH3 is CSPWL076.** **6. Fixed system stuck at 0xB2 when plugging BPS with MM mode.**

	7. **Updated AMITSE module for AMI SA50216 Security Advisory(LogoFAIL Vulnerability) to address CVE-2023-39538(7.5, High) and CVE-2023-39539(7.5, High) security issues.** 8. **Exposed "Pre-boot DMA Protection".** 9. **Updated code per system spec rev 5.**
New features	**None**
Fixes	1. **Resolved how the KMS configuration could not be preserved after load BIOS default.** 2. **Fixed how the HostInterface On/Off test will drop in four times in UEFI Shell. (Refer to EagleStream SVN3178.)** 3. **Displayed dynamic gateway IPV6 address as "::::::" on BIOS setup if dynamic router info set count was 0.** 4. **Displayed static gateway IPV6 address as "::::::" on BIOS setup if could not get valid gateway IPV6 address through IPMI.** 5. **Fixed bug where SMBIOS type 9 slot 5 entry would be deleted in 1U systems.**

Release Notes from Previous Release(s)

1.5 SPS: 4.4.4.301 (4/25/2023)

1. *Updated BIOS revision to 1.5.*
2. *Updated 5.22_WhitleyCrb_0ACMS_ICX_075 Intel 2023.2 IPU-PV*
3. *Pulled high GPP_C10_FM_PCH_SATA_RAID_KEY first before VROC key detection.*
4. *Fine-tuned VROC key detection function.*
5. *No boot option for single HDD under RAID mode.*
6. *Added ECM RNDIS support.*
7. *Fixed system hangs on 0xA9 after setting MMCFG base to 1.5G and 1.75G.*
8. *Fixed that the SUM TC: 2020 test fail problem.*

1.4a (11/24/2022)

1. *Updated 5.22_WhitleyCrb_0ACMS_ICX_73 Intel BKCWW40 PLR3 OOB. Please check header for firmware revisions.*
2. *Updated VROC SATA/sSATA EFI driver to VROC PreOS v7.8.0.1012 to address Intel Virtual RAID on CPU (VROC): Data Loss Exposure Due to RAID 5 TRIM Support document #737276*
3. *Added "CSM Support" setup item into SMCISBForm page.*
4. *Filter Dynamic TCG Security Pages to patch SUM ChangeBiosCfg failed problem*
5. *Enhanced get VPD data routines for E810.*
6. *Supports IPMI PXE boot to all LAN port feature for both Legacy and UEFI PXE.*
7. *Applied workaround to fix Linux OS show incorrect CPU max freq issue.*
8. *Updated SmcOOB to the version "_SMCOOBV1.01.25_" to fix the unexpected system-reseting when loading NVRAM defaults.*
9. *Exposed Link Retrain per port, exposed MCTP for CPU1 slot1 and CPU2 slot2 in BIOS.*
10. *If chassis type of FRU0 is not 1(other) or 2(unknown), sync it to SMBIOS type 3.*
11. *Updated Intel Server Platform Services for Whitley Server Platforms IPU2023.1 4.4.4.301*
12. *Fixed SUM ChangeBiosCfg command cannot update PchSetup variable related BIOS items issue.*

1.1 (5/7/2021)

1. *Set default Boot Guard profile to 5.*
2. *Updated Intel BKCWW17 2021 PV MR1.*
3. *Set all OPROM control items to Legacy when boot mode is set to Dual.*
4. *Updated CPLD Signature table 101 and tool to 1.30.24 for CPLD Signature.*
5. *Extended memory DIMM serial number information (Samsung, Micron, Hynix).*
6. *Fixed problem of T-states always showing 15 levels even when T-state is disabled.*
7. *Fixed missing offboard output in Setup if limited to 4G in Non-EFI mode.*
8. *Fixed failure of Microsoft HLK certification and TPM 2.0 UEFI Preboot Interface Test on Microsoft Server 2019.*
9. *Fixed problem with a CPU exception.*
10. *Fixed failure to hide the SmcSecureErase setup page when no HDD devices are plugged in.*
11. *Corrected display of UEFI OS boot option name in BIOS setup.*
12. *Fixed failure of Secure Boot Append/Update Keys.*
13. *Fixed inability to upload all OOB files on the first BMC boot.*
14. *Corrected memory device number in SMBIOS type 16.*

15. *Corrected iSCSI Configuration page.*
16. *Set DIMM size to recalibrate when rank is disabled.*
17. *Fixed the issue of system hanging after executing sum -c EraseOAKey or afuefi /OAD.*

_____ _____

Product Manager *Date*