BIOS Release Notes Form

Product Name	**X12DPT-PT6**
Release Version	**1.1a**
Release Date	**9/2/2021**
Build Date	**9/2/2021**
Previous Version	**1.1**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated BIOS revision to 1.1a.** **2. Updated 5.22_WhitleyCrb_0ACMS_ICX_067 Intel BKCWW32 2021 PV MR5.** **3. Updated BIOS/SINIT ACM 1.0.D.** **4. Set TXT to require NV indexes to TPM to prevent TPM 1.2/2.0 from disappearing when enabling Intel "TXT Support" without provisioning Intel.** **5. Changed "Hard Drive Security Frozen" default setting to disabled.** **6. Added support for SUM upload/delete HTTPS TLS certificate.** **7. Disabled support for EFI iSCSI.** **8. Patched case of BMC Redfish Host Interface being named ethX when CDN is disabled under Linux OS.** **9. Modified Me version strings and removed the "Manufacturer ID" string.**

New features	**N/A**
Fixes	**1. Fixed failure of WHLK TPM 2.0 Supplemental test.** **2. Fixed inability to preserve SGX settings after updating BIOS.** **3. Corrected firmware version and vendor on Trusted Computing page.**

Release Notes from Previous Release(s)

1.1 (7/8/2021)

1. Updated 5.22_WhitleyCrb_0ACMS_ICX_066_BETA Intel BKCWW24 2021 PV MR4.
2. Updated Dx/Mx microcode from Intel-Generic-Microcode-20210701_NDA.
3. Updated SATA/sSATA EFI driver to VROC PreOS v7.6.0.1012.