BIOS Release Notes Form

Product Name	**X14DBT-FAP**
Release Version	**1.3**
Release Date	**04/01/2025**
Previous Version	**1.0**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Updated code base to 5.35_0ACQZ_3544P36_GNRAP_GNRSP_SRFSP_073_BETA for BKCWW12 GNR MR1.** **2. Updated Birch Stream Granite Rapids SP - MR1 OOB Candidate BKC.** **3. Updated Secure Boot DBX to address the AMI SA50300 (CVE-2024-7344\CVE-2023-24932 (8.2 High/6.7 Middle)) security issue.** **4. Implemented the TPM EK public certificate feature.** **5. Removed the warning message, "Crystal Ridge is not support."** **6. Fixed the CPU one core drop issue.** **7. Exposed the "Enable SAF" item.** **8. Enhanced SMC_STYLE_CPU_CORES_ENABLE function by Die Count.** **9. Avoided how the mapped-out DIMM could not recover after an AC cycle.**

	10. When enabling block SID, set AUTO_ACCEPT_PPI to avoid having to wait for user acceptance to continue. 11. Implemented SmcTpmInfo module for the TPM Redfish MeasurementSet feature. 12. Updated the built-in SuperDiag to ECO candidate 1.10.1 version, based on GIT_2bc33501019e721aa4722f4269f0e2bfbcf5c34c.
New features	**None**
Fixes	1. The attribute 'MaxTDPWatts' could not appear at URI '/redfish/v1/Systems/1/Processors/[number].' 2. Fixed the system hang after executing PPR. 3. Fixed the issue where some BIOS items' default value could not be changed.