BIOS Release Notes Form

Product Name	**X12STL-F**
Release Version	**1.4a**
Release Date	**3/6/2023**
Build Date	**3/6/2023**
Previous Version	**1.4**
Update Category	**Recommended**
Dependencies	**None**
Important Notes	**None**
Enhancements	**1. Update BIOS version to 1.4a.**
New features	**None**
Fixes	**1. Patch to fix the PCH chip that causes the USB 0C problem.**

Release Notes from Previous Release(s)

1.4 (12/22/2022)

1. *Updated BIOS version to 1.4.*
2. *Updated Microcode A0671 to 0x57 and A0653 to 0xF4 per IPU 2023.1 Processor Advisory INTEL-TA-00767 to address CVE-2022-38090 (6.0 Medium).*
3. *Updated ACM version to 1.14.46 (20220819) per IPU 2023.1 Processor Advisory INTEL-TA-00767 to address CVE-2022-30704 (7.2 High).*
4. *Updated the SPS ME firmware to SPS_E3_06.00.03.309.0 per IPU 2023.1 Processor Advisory INTEL-TA-00718 to address CVE-2022-36794 (6.0 Medium).*
5. *Updated EfiOsBootOptionNames and relevant dependencies for the Security update.*
6. *Modified the options of "Gen3 ASPM Control" and "Gen3 ASPM" match loading defaults by pressing F3.*

1.2 (7/11/2022)

1. *Applied a patch based on AMI Customer Advisory document UefiNetworkStack Aptio 5.x SA50110.*
2. *Changed the text string "Security Erase Configuration" to "SMCI Security Erase Configuration."*
3. *Filtered the dynamic TCG security pages to patch the SUM ChangeBiosCfg failed problem.*
4. *Updated BIOS ACM and SINIT ACM to 1.14.39 (20211214) for 2022.1 IPU - BIOS Advisory. INTEL-TA-00601 addresses CVE-2021-33123 (8.2 High), CVE-2021-33124 (7.5 High) and CVE-2021-33103 (7.5 High).*
5. *Enabled SMBIOS chassis type to be the same as the FRU0 chassis type.*
6. *Changed the FRU0 chassis type to SMBIOS type 3 if it is not 1 or 2.*
7. *Updated AHCI driver from version 23 to version 28.*
8. *Enabled boot option for single HDD under RAID mode.*
9. *Updated Microcode to 0x54 per IPU 2022.2 Processor Advisory INTEL-TA-00657 to address CVE-2022-21233 (6.0 Medium).*
10. *Updated the root complex chipset with source code label 17 (5.22_1AXCT_RC0B.01.34.60_017).*
11. *Updated SMCOOB to 2.00.14.*
12. *Added the current boot device name in the SUM OOB configuration.*
13. *Fixed an error when an unknown device is installed and Intel® TXT is enabled.*
14. *Fixed the setup options of Enable Root Port, Max Link Speed, and ASPM of PEG Port Configuration.*
15. *Fixed the boot order displayed after using the AMIBCP tool.*
16. *Fixed the channel per DIMM displayed in the event log for DIMMB1.*

1.0a (11/18/2022)

1. *Added Intel PEG port width drop workaround and PEG port speed drop workaround.*
2. *Added Intel IPS #00641060 patch to support disabling of AVX/AVX3. Added AVX and AVX3 setup items.*
3. *Updated Microcode M02A0671_0000004C.*
4. *Added LAN1 and LAN2 Support items in PCIe/PCI/PnP Configuration.*
5. *Fixed an issue that when disabling BMC IPv6 Support in the BIOS, the IPv6 Address Status will show "Disabled" instead of "_".*
6. *Fixed system Recovery hang on 0x94 after BIOS crash under Dual mode.*
7. *Fixed serial number in SMBIOS type 17, as it loses bytes when using Samsung DDR4 memory.*
8. *Fixed SMCIPMITOOL/IPMICFG where it can't set persistent boot under DUAL mode, and Legacy mode through IPMI Boot Flag Command.*

9. *Fixed susceptibility to DDR4 Rowhammer attacks.*