EagleStream/SPR Platform CRB BIOS Release Notes

August 5th, 2020
BIOS Revision: 40D08

Legal Information

Disclaimer

Intel attempts to release Server BIOS binaries, under NDA for testing on supported CRBs that adhere to the same security requirements as should be used in production. However, some BIOS differences exist. The differences, which do not adhere to security requirements, that should be addressed before releasing a product based on for this release are listed below:

1. GPIO lock: The current CRB BIOS binary leaves the GPIOs unlocked, with a setup control to change the default. In a true production BIOS, the GPIOs are locked and no setup control to override exists.

2. SPI Lock: The current CRB BIOS binary leaves SPI unlocked to allow ease of upgrade in the field using nonproduction applications to upgrade CRBS to non-production binaries. In a true production BIOS, SPI is locked. In particular, the SPI flash descriptor permissions should be set to least privilege.

3. Runtime Variables: The current CRB BIOS binary defines Several PCDs as Dynamic HII PCDs such that validation has maximum flexibility in debug by offering setup control over these features. In a true production BIOS, these PCDs should be static PCDs configured at build time.

4. SWSMI Interface: The current CRB BIOS binary exposes several SWSMI functions to support ease of configuration by internal validation applications. The source code to these functions has not been included, though they are present in the binary. In a true production BIOS, these interfaces should not exist.

Contents

BKC to BIOS mapping

BKC release	IFWI image	BIOS revision	Microcode	SPS FW	BIOSACM	SINIT
WW32'20	2020.31.3.04	40D08	m_97_806f0_8a0001f0	E5_06.00.00.102.0	Debug_TR, v0.5.4	Debug_TR, v0.5.4
WW18'20	2020.16.4.01	32D23	n/a	E5_06.00.00.044.0	Debug_TR, v0.5.0_ENG	Debug_TR, v0.5.0_ENG
Ww14'20	2020.12.4.04	30D16	n/a	E5_06.00.00.044.0	Debug_TR, v0.5.0_ENG	Debug_TR, v0.5.0_ENG
Ww10'20	2020.08.04.02	28D13	n/a	E5_06.00.00.56.0	Debug_TR, v0.5.0_ENG	Debug_TR, v0.5.0_ENG
Ww07'20	2020.05.06.01	27D15	n/a	E5_06.00.00.56.0	Debug_TR, v0.3.1_ENG	Debug_TR, v0.3.0_ENG
Ww01'20	2019.52.4.02	23D31	n/a	E5_06.00.00.52.0	Debug_TR, v0.3.1_ENG	Debug_TR, v0.3.0_ENG
Ww48'19	2019.46.5.02	21D22	n/a	E5_06.00.00.037.0	Debug_TR v0.3.0_ENG	Debug_TR v0.3.0_ENG
WW46'19	2019.44.4.02	20D14	n/a	E5_06.00.00.037.0	Debug_TR v0.3.0_ENG	Debug_TR v0.3.0_ENG
WW42'19	2019.39.4.02	18D10	n/a	E5_05.00.00.030.0	Debug_TR v0.3.0_ENG	Debug_TR v0.3.0_ENG

Potential issues

**Note: below table lists sightings that are under investigation*

id	title	Owning forum
1508228778	[EGS-FW_EVAL][SPR A0 PO] SUT boot hang with BIOS version greater than 0040.D12	UEFI_SYSDEBUG-PCH
1508231303	[EGS-FW_EVAL][SPR A0 PO]Serial port output is incorrect when select BIOS option and check BIOS option's value in BIOS setup UI	UEFI_SYSDEBUG-RAS
1508231364	[EGS-FW_EVAL][SPR silicon] 2S platform boot hang with BIOS 40.D18 (GP fault while writing SEAMRR 0x1401)	UEFI_SYSDEBUG-Security
14012169936	SPR 4S bringup BIOS hang	UEFI_SYSDEBUG-PCH
14012148576	[TXT] VTd Bus decoding is failing on 2S configuration preventing trusted boot	PLATF_SYSDEBUG_ACM
14012172060	[SPR] BIOS is not programming CXPSMB segment/source mapping correctly	UEFI_SYSDEBUG-IIO
16011460953	[SPRHBM EMU] Issue when running in HBM Flat Mode configuration on srvr10nm_24c_mdfsfix_062120-002 (4 Die)	
18012175615	[EGS][Security][TDX][A0] SEAMRR configuration mPservices in BIOS causes #UD	UEFI_SYSDEBUG-Security
22010732361	[SPR A0 PO][SGX] VAPA with SGX causes SGX disable	UEFI_SYSDEBUG-Security
1307811302	[EBG A0] Cannot program IO traps because PSTH P2SB endpoint is already disabled in EPMASK[0-7]	UEFI_SYSDEBUG-PCH
1507885787	[EGS-FW_EVAL][SPR]SUT show incorrect frequency in memory topology with 1S-1D-WB-DDRT.simics script	UEFI_SYSDEBUG-DDR
1507937431	[EGS-FW_EVAL][SPR] SUT show fatal error when resume from s3	UEFI_SYSDEBUG-DDR
1507987499	[EGS-FW_EVAL][SPR] SUT reboot will hang after enable BIOS knob “attempt fast cold boot” with full memory configuration.	UEFI_SYSDEBUG-DDR
1508019783	[EGS-FW_EVAL][SPR A0 PO] Mix DIMM 16G&32G display FatalError	UEFI_SYSDEBUG-DDR
1508037505	[EBG] EBG clean up for CDF_SC_FLAG flag	UEFI_SYSDEBUG-PCH
1508171793	[EGS-FW_EVAL][SPR silicon]Register value not match when set Link Frequency to 14.4GB/S	UEFI_SYSDEBUG-KTI
1508193015	[FW_Eval][IP_Uncore][HBM]ha_ad_credits_cfg&CR_ha_bl_credits_cfg & CR_ha_bl_credits1_cfg was not programmed correct on 1S-1LM-HBM-SNC4 configuration	UEFI_SYSDEBUG-KTI
1508207574	[EGS-FW_EVAL][SPR Emulation] 2LM test gets to HANG with Trunk BIOS 39.D20	UEFI_SYSDEBUG-Platform
1508210052	[FW_EVAL][IP_RAS] Address decode failed for full mirror scenario.	UEFI_SYSDEBUG-RAS

1508225104	[SPR 8S3L SPW] Not enough available heap for requested allocation	UEFI_SYSDEBUG-DDR
1508225277	[FW_EVAL][IP_MRC] Register cmpl_to_data_delay.cmpl_program_delay is programed with 4 rather than 8 for DDR5	UEFI_SYSDEBUG-DDR
1508228759	EBG GPIO definition overlap	UEFI_SYSDEBUG-PCH
1508228760	[FW_EVAL][IP_RAS] ADDDC can not pair to any NonFailedRank except itself	UEFI_SYSDEBUG-RAS
1508232843	[FW_EVAL][IP_RAS] The 3rd parameter of GetChannelErrorInfo( ) function in UpdateEnhancedDimmErrRecord( ) should not be 'FALSE'.	UEFI_SYSDEBUG-RAS
1707211241	[SPR A0 PO] KFIR fails to train in 3226.d33 or later	UEFI_SYSDEBUG-PCH
1707215337	[SPR A0 PO] Rx Dq Dqs should fatal error when no eye is found across all settings	UEFI_SYSDEBUG-DDR
14011685993	SiSysDbg FWD: MCTP broadcast responses sent by OOB MSM are not reaching destination - CSME	UEFI_SYSDEBUG-ME
14011731892	[KW] Resolve KW errors (CR)	UEFI_SYSDEBUG-CR_Memory_Map
14011841501	[SPR A0 PO] 8S build hangs after gEfiEndOfPeiSignalPpiGuid	UEFI_SYSDEBUG-Platform
14011867917	[EGS SPR A0 PO] [PLATPO] [Archer City] [VROC] RAID Menu not visible in BIOS->EDKII Menu	UEFI_SYSDEBUG-PCH
14011868152	[EGS SPR A0 PO] [PLATPO] [Archer City] Can't find VMD device in menu "Intel Virtual RAID on CPU ".	UEFI_SYSDEBUG-IIO
14011918211	[SPR] BIOS is not configuring SLOTCTL correctly after hot plug is enabled	UEFI_SYSDEBUG-IIO
14011936924	PARA is not supported by GetSetDcaVrefDdrt2	UEFI_SYSDEBUG-DDR
14012058549	[SPR-EBG A0][ADR]: Missing BIOS Programming for ADR Registers(ADR_PLT_ACK_EN & GPIO_B_SEL registers)	UEFI_SYSDEBUG-PCH
14012114561	[SPR][NTB]:NTB Link does not train when connected to port 2H,3H,4H,5H	UEFI_SYSDEBUG-IIO
16011441689	[SPRHBM EMU] Memicals 2LM(HBM-NM; DDR-FM) test failing due MCA error	
22010529063	[SPR] Incorrect implementation of IsOppSrEnabled	UEFI_SYSDEBUG-DDR
22011065810	DDRT 2.0: Req training does not handle lane reversal and dimm slot 1 correctly	UEFI_SYSDEBUG-DDR
22011117822	BIOS should not access CXPSMB/MCSMBUS after it was enabled	UEFI_SYSDEBUG-IIO
22011197685	BIOS overwrite to 0xb40007d0 too early and doesn't stick	
22011207273	[SPR A0 VV] DDR5 CAP Programming for the tpar_recov field incorrect	UEFI_SYSDEBUG-DDR
1507695722	RxSamplerLo and RxSamplerHi are no need to be within #ifdef SPR_HOST	UEFI_SYSDEBUG-DDR

1507867158	[EGS-FW_EVAL][SPR]Cannot boot to BIOS Setup after change “Multi-Threaded MRC” to enable and do save and reset function	UEFI_SYSDEBUG-Security
1507911936	[SPR]]system will hang after bootscenario negative test (remove timestamp/keyblob) and reboot	UEFI_SYSDEBUG-Security
1507960390	[EGS-FW_EVAL][SPR A0 PO] Cannot boot to BIOS Setup when set knob “Write Preamble TCLK” to “4TCLK”	UEFI_SYSDEBUG-DDR
1508164693	[SPR] ReadDbMr() always returns 0 when reading MR from DB	UEFI_SYSDEBUG-DDR
1508171490	[SPR A0 PO] The DB DFE margin result is too large for data lanes except for ECC lanes.	UEFI_SYSDEBUG-DDR
1508204458	[EGS-FW_EVAL][SPR] DDRT dimm should show CPS-DIMM but show DCPMM-DIMM	UEFI_SYSDEBUG-DDR
1508213464	[EGS][Security][TBoot] After Enable TXT, TXT measured launched FALSE In Tboot OS.	UEFI_SYSDEBUG-Security
1606812563	[VPQA]EGS BIOS hung after changes to UPI menu	
1707097466	[SPR] DDRIO settings not returned to original value at the end of DCS training	UEFI_SYSDEBUG-DDR
1707198534	[SPR A0 PO] Swizzle Discovery Display does not work for x4 DIMMs	UEFI_SYSDEBUG-DDR
1707229928	[SPR A0 PO]Mixed config is training DIMM 1 DCS on a 1DPC Channel	UEFI_SYSDEBUG-DDR
1707237263	SPR Mem CSR access functions adding 600ns latency	UEFI_SYSDEBUG-DDR
1707259181	Enable FMMT tool to be able to find and replace the microcode FFS in gen2 platforms.	UEFI_SYSDEBUG-Platform
14010928093	[SPR] DFE training passes SendMrwPda invalid values for Dram	UEFI_SYSDEBUG-DDR
14011251188	[SPR A0 PO] DQ Swizzle discovery is not turning off inverted pattern on the last bit as a cleanup step	UEFI_SYSDEBUG-DDR
14011271280	[SPR A0 PO] DCA DFE Prints are printing 512 samples instead of the number of tests.	UEFI_SYSDEBUG-DDR
14011365624	RC report EWL Type-3 warnings with wrong major/minor codes	UEFI_SYSDEBUG-DDR
14011418676	[SPR A0 PO] Between tap settings not setting the per bit coefficients to the trained value of previous tap setting.	UEFI_SYSDEBUG-DDR
14011430453	[SPR A0 PO] Final trained settings need to be printed in Read Dfe.	UEFI_SYSDEBUG-DDR
14011486247	[SPR A0 PO] Xover values are printed as the same values across MCs	UEFI_SYSDEBUG-DDR
14011491303	[SPR A0 PO] PMIC registers 0x4d and 0x4e being set to 0 which is spec violation	UEFI_SYSDEBUG-DDR
14011503509	[SPR A0 PO] Write Leveling is setting CWL_ADJ twice, and the second loop is programming DDRT2 CWL_ADJ incorrectly	UEFI_SYSDEBUG-DDR
14011635331	[EBG A0 CLX VV] eSPI LGMR1 and LGIR1 registers are not being programmed by BIOS	UEFI_SYSDEBUG-PCH

14011726207	[SPR A0 PO] Backside Rx Dqs LRDIMM training fails when all channels are populated 2DPC	UEFI_SYSDEBUG-DDR
14011785666	[SPR A0 PO] MRE training failing on a fuly populated LRDIMM system.	UEFI_SYSDEBUG-DDR
14011799742	[SPR A0 PO] MRD training failing on a fully populated LRDIMM system.	UEFI_SYSDEBUG-DDR
14011847267	[CXL] _CID of Host Bridge Created for CXL Devices must be "PNP0A03"	UEFI_SYSDEBUG-KTI
14011942969	[SPR A0 PO] KIT Table DQ Vref not being set correctly on back side.	UEFI_SYSDEBUG-DDR
14011955535	[SPR A0] Socket1 NPK bars are not getting programmed	UEFI_SYSDEBUG-IIO
14011997195	[SPR A0 PO] DB DFE CPGC programming should target rank0	UEFI_SYSDEBUG-DDR
14012022306	EagleStreamRpPkg: Remove third-party driver from external builds	UEFI_SYSDEBUG-Platform
14012022712	EagleStreamRpPkg: Remove obsolete SPS tool components	UEFI_SYSDEBUG-Platform
14012029353	[SPR] SEAMRR range reported as available (not reserved)	UEFI_SYSDEBUG-Security
14012147029	[SPR A0 VVR] erruncsts.UR bit is not cleared after ANFES is generated in several DINO HCx IPs	UEFI_SYSDEBUG-RAS
14012172850	[SPR A0 PO] CAS Latency is not programmed for all DRAMs	UEFI_SYSDEBUG-DDR
22010035913	[BiosGuard] Cleanup ServerPlatformPkg references in ServerSecurityPackage Module INF files	UEFI_SYSDEBUG-Security
22010036012	[CBnT] Cleanup ServerPlatformPkg references in ServerSecurityPackage Module INF files	UEFI_SYSDEBUG-Security
22010504907	[SPR A0 PO] TxVref GetSet not returning to original value in marginsweep when in NonPDA mode.	UEFI_SYSDEBUG-DDR
22010539685	[SPR A0 PO] Taps for subch B not programmed correctly	UEFI_SYSDEBUG-DDR
22010821156	Bios flows accessing LT MMIO Region without check for LtEnabled	UEFI_SYSDEBUG-Security
22010823460	SpiCommon.c runtime stall routine calls non-runtime-safe code	UEFI_SYSDEBUG-PCH
22011049373	[SPR]Read DQ Dqs sweep headers should print even if CH0 is not populated.	UEFI_SYSDEBUG-DDR
22011130269	[CXL] PCIe Host Bridge that is sibling to CXL Host Bridge (with attached CXL RCIEPs) Yellowbangs	UEFI_SYSDEBUG-KTI
22011170510	[SPR A0 PO] Read DQDQS Pre Dfe 2D Centering on LRDIMM has 0 margins on all sweep settings	UEFI_SYSDEBUG-DDR

22011183008	[SPR][PCIE] IIO DFX Configuration->Socket<n> Configuration->Port [x]->Gen5 Override Mode-> Test Card->Laguna does not set the EQ override	UEFI_SYSDEBUG-IIO
22011187659	[SPR A0 PO] LRDIMM: Incorrect pattern for DWL	UEFI_SYSDEBUG-DDR
22011208141	[SPR] Warm reset is failing on Bios k:\intel\CpRcPkg\Library\BaseDdr5CoreLib\MemJedecDdr5.c: 443	UEFI_SYSDEBUG-DDR
1508199437	[FW_EVAL][IP_MRC] Fatal Error in Knob: Disable ECC	UEFI_SYSDEBUG-DDR

BIOS Releases

**Note: this section lists issue fixes in each BIOS revision*

BIOS revision: 0040.D.08

Please see gitlog.

BIOS revision: 0032.D.23

Please see gitlog.

BIOS revision: 0030.D.16

Please see gitlog.

BIOS revision: 0028.D.13

Please see gitlog.

BIOS revision: 0027.D.15

Please see gitlog.

BIOS revision: 0023.D.31

Please see gitlog.

BIOS revision: 0021.D.22

Please see gitlog.

BIOS revision: 0020.D.14

Please see gitlog.

BIOS revision: 0018.D.10

Please see gitlog.

CRB BIOS errata

This section lists permanent errata for Intel CRB BIOS

No.	Description
1.	
2.	

END OF DOCUMENT