BIOS Update Release Notes

PRODUCTS: DQ965CO, DQ965GF, DQ965WC (Standard BIOS)

BIOS Version 5953

About This Release:

- July 31, 2007
- CO96510J.86A.5953.2007.0730.2059
- VBIOS info: Build Number: 1471 PC 14.27 03/23/2007 16:50:31.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.1.1001
- SATA AHCI info: Version UPSD src 04-20-2007
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.50
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Fixed "Validate the Consistency of the TCPA EventLog" failure with Windows* Logo Kit 1.0c TPM BIOS Interface Logo Test.
- Added ITK Data Var Type 3 to store VAREQ variable.
- Fixed issue where flashing a large BMP Logo caused inability to reflash and possibly not boot.

BIOS Version 5947

About This Release:

- July 25, 2007
- CO96510J.86A.5947.2007.0725.1741
- VBIOS info: Build Number: 1471 PC 14.27 03/23/2007 16:50:31.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.1.1001
- SATA AHCI info: Version UPSD src 04-20-2007
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.50
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Updated fix for issue where ME WOL from S5/S3 wake the whole system instead of just ME.
- Fixed ME page shows junk while press <F9> to load default.
- Fixed issue where Quad core CPU not able to run in single processor mode.
- Workaround an intermittent failure seen with EFI_VARIABLE in Windows environment.
- Fixed issue where language selection and language display are not matched after user pressed F9/loaded default in BIOS setup.
- Added capability to override debug patches even if the patch version is lesser than the current version.
- Fix for initializing OemDefault variable to proper size.
- Fixed the problem where disabling USB legacy support hangs the legacy free system during POST.
- Updated processor support.
- Fixed issue where the BIOS was potentially using all processor variable MTRRs.

- Reverted back the ME FW version to 2.1.3.1031 production signed.
- Fixed Microsoft Vista* 64-bit not able to install or boot with certain processor.
- Added additional warning message after AMT reset to default.
- Improved S3 resume time.
- Added successful message after AMT reset to default on Maintenance Page.
- Fixed DMI Memory Slot Location ID Doesn't Match Motherboard Markings.
- Fixed issue where "Single Processor Mode" setup option not working.
- Fixed issue where BIOS incorrectly report AMT setup error during POST.
- Fixed issue where ME WOL from S5/S3 wake the whole system instead of just ME.
- Added QST support for new processors.
- Added support for new CK505 clock, SLG845168BT.
- Fixed issue where ME_ENABLE bit in CK505 not set before ME init during S3 resume.
- Fixed a problem where the system would sometimes hang when the CMP was disabled.
- Fixed issue where USB keyboards were not usable during option ROMs initialization.
- Fixed the problem where disabling USB legacy support hanged the legacy free system during POST.
- Fixed unable to boot from local HDD after using IDE-R session.

BIOS Version 5931

About This Release:

- June 15, 2007
- CO96510J.86A.5931.2007.0614.2236
- VBIOS info: Build Number: 1471 PC 14.27 03/23/2007 16:50:31.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.1.1001
- SATA AHCI info: Version UPSD src 04-20-2007
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.50
- ME firmware build: 2.2.0.1028 production signed.

New Fixes/Features:

- Fixed OCUR support.
- Fixed Microsoft* OEM Activation 2.0 support.
- Reverted back the CPU module from Baseline 8.6 to Baseline 8.0 to avoid some CPU issues.
- Added messages for USB key provisioning.
- Fixed ME "End of DRAM Respond" error when the board is first power up.
- Fixed issue where some USB 2.0 boot devices become disabled late in POST or at boot.
- Fixed issue where the change in BIOS language does not take place cleanly for many cases.
- Fixed issue where all the information (including ME version) in "Additional System Information" page is lost, after the language is changed.
- Fix issue where UUID field is not implemented/removed completely in "Additional System Information" page.

- Removed provisioning related command line options from Express BIOS update.
- Corrected Vendor Specific ID for AMT.
- Fixed issue where Language selection and language display mismatch after press Ctrl+Alt+Del.
- PET/AMT Event Log: Added Chassis Intrusion message.
- Added support for PCIE checking for CK505 clock.
- Updated MRC to version 1.7.
- Fixed issue where language selection and language display are not matched after user pressed F9/loaded default in BIOS setup.
- Fixed issue where language display in BIOS setup is not changed according to BIOS setup variable.
- Fixed a potential VPD corruption issue.
- Fixed issue where system with 4GB memory boot very slow the first time after SPI fresh burned.
- Updated Intel(R) ME Firmware to 2.2.0.1028.
- Synch up the CPU module from Baseline 8.0 to Baseline 8.6.
- RAID option rom: Intel(R) RAID for SATA - v6.1.1.1001.
- Added support for Winbond* W25X16 16Mb SPI part for ICH8.
- Fixed issue where variable was failing to update correctly from Windows application.
- PET/AMT Event Log: Added more detail on BIOS boot progress.
- Implement dynamic detection method for SRC0_SEL setting.
- Lock SPI flash descriptor for production BIOS.
- Fixed F9 Load Default action from Intel(R) ME page does not load correct defaults.
- Added force On-board LAN Device setup option to Maintenance mode.
- Removed ME debug code that produced ME beep codes during POST.
- Fixed resource allocation issues with PCI cards with multiple P2P bridges.
- Changed the HDD pre-delay option's stepping style.
- Fixed issue where certain USB bar code scanners would drop a single character if used under USB Legacy.
- Video BIOS Build Number: 1471 PC 14.27 03/23/2007 16:50:31.
- Added BuildVariables to allow TURN_OFF_BIOS_WP flag to take affect.
- Fixed issue where incorrect resource being allocated to PCI/PCIe devices when ISA_EN bit enabled in the bridge.
- Fixed Vista* x64 not able to install issue.
- Removed fix for issue where system would run slow under Windows XP with 4 GB of RAM and certain PCI Express Graphics cards.
- Updated processor support.

BIOS Version 5882

About This Release:

- April 13, 2007
- CO96510J.86A.5882.2007.0413.0100
- VBIOS info: Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Updated processor support.
- Changed the manufacturing SATA Type default to follow customer default.
- Fixed issue where incorrect resource being allocated to PCI/PCIe devices when ISA_EN bit enabled in the bridge.
- Fixed issue where system would run slow with 4 GB of RAM and certain PCI Express Graphics cards.
- Removed an 8 second delay from the ACHI option ROM to speed up POST.
- Added more detail on BIOS boot progress for PET/AMT Event Log.
- Fixed false alarm event for User is Entering Setup for PET/AMT Event Log.
- Fixed false alarm event for Keyboard Error for PET/AMT Event Log.
- Removed false alarm event for AmtBx Error for PET/AMT Event Log.

BIOS Version 5874

About This Release:

- April 06, 2007
- CO96510J.86A.5874.2007.0405.2356
- VBIOS info: Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Change SATA Type default in MFG mode to AHCI if the board capable for AHCI/RAID.
- Fixed Audio Code subsystem ID problem after resuming S3.
- Removed false alarm event for AmtBx Error in PET/AMT event log.
- Fixed false alarm event for Keyboard Error in PET/AMT event log.
- Fixed false alarm event for User is Entering Setup in PET/AMT event log.
- Added support to reserve an exclusive memory region for LT heap & SINIT + Additional enhancements.
- Fixed priority issue in Advance Boot Mode when Legacy Floppy is installed without a media.
- Fixed issue certain processors have boot problem to Microsoft* Windows* Vista.
- Changed the display string in Hardware Monitoring page from "+1.5V" to "MCH Vcc".
- Fixed issue where flashing a large .BMP Logo caused inability to reflash and possibly not boot.
- Fixed issue where certain keyboard does not work with USB Legacy support.
- Fixed issue where user needs to press power button twice to power on the board when WOL set to disable.
- Fixed WOL from G3 feature not working issue.
- Updated processor support.

BIOS Version 5869

About This Release:

- March 27, 2007

- CO96510J.86A.5869.2007.0327.0132
- VBIOS info: Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Fixed boot issue with certain processors.
- Fixed issue where certain keyboard does not work with USB Legacy support.
- Fixed issue where user needs to press power button twice to power on the system when Wake On LAN from S5 is set to "Power Off".
- Fixed boot order for SCSI HDD.
- Fixed priority issue in Advance Boot Mode when Legacy Floppy is installed without a media.
- Updated processor support.
- Fixed System hang during IDER boot with USB bootable device connected.
- Fixed issue where CD-ROM retries were not functioning after the "No bootable device -- insert boot disk and press any key" message.
- Fixed issue where certain USB bar code scanners would drop a single character if used under USB Legacy.
- Add EIT ACPI OpRegion.

BIOS Version 5858

About This Release:

- March 14, 2007
- CO96510J.86A.5858.2007.0314.0016
- VBIOS info: Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.3.1031 production signed.

New Fixes/Features:

- Fixed an issue where LAN lost power during S3 if Wake On LAN from S5 is set to "Power Off".
- Fixed system hang during IDER boot with USB bootable device connected.
- Fixed issue where system would hang booting Windows* XP with OEM Activation 2.0 data programmed, EIST enabled, and certain processor installed in the system.
- Add EIT ACPI Device INT5400 for VA2.6 and later Installer, ACPI OpRegion BIOS Smm handler.
- Fixed issue where the SOL terminal is not functional on the first reboot after AMT SOL is activated.
- Fixed handling of platform power management after AC-Loss.
- Workaround issue where system not able to boot to Microsoft Windows Vista* when 4GB memory installed.
- Added VT Enable/Disable Callback causing Global Reset when changing VT state.
- Allow VA LVMM Installer to set the BIOS Setup VA BA Boot Policy.
- Fixed EIT changing Video mode when in manufacturing mode.

BIOS Version 5844

About This Release:

- March 2, 2007
- CO96510J.86A.5844.2007.0302.0258
- VBIOS info: Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.3.1031 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Update video BIOS to Build Number: 1436 PC 14.21 02/05/2007 17:31:04.
- Removed handling of platform power management after AC-Loss for Intel® AMT support fix.
- Updated processor support.
- Added support to generate event log if AA# not programmed correctly.
- Updated ME FW to v2.1.3.1031.
- Fixed F9 Load Default action from Intel(R) ME page does not load correct defaults.

BIOS Version 5840

About This Release:

- February 26, 2007
- CO96510J.86A.5840.2007.0225.2142
- VBIOS info: Build Number: 1402 PC 14.21 11/30/2006 12:21:54.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.0.1028 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Added programming of PCI Subsystem Vendor ID and Subsystem ID for the PCIe Graphics bridge.
- Fixed handling of platform power management after AC-Loss for Intel® AMT support.
- Removed USB2.0 Enable/Disable setup option.
- Added help text for fan control questions.

- Modified ACPI OSFR support so that the Microsoft* Reference Block is now an optional parameter.

BIOS Version 5803

About This Release:

- February 16, 2007
- CO96510J.86A.5803.2007.0215.1915
- VBIOS info: Build Number: 1402 PC 14.21 11/30/2006 12:21:54.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.0.1028 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Fixed issue where "Flex Modules" cannot be edited using ITK.
- Added new SKU AA number.

BIOS Version 5773

About This Release:

- February 6, 2007
- CO96510J.86A.5773.2007.0206.0046
- VBIOS info: Build Number: 1402 PC 14.21 11/30/2006 12:21:54.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.0.1028 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Hide AHCI option ROM text when system is not running in RAID mode.
- Modified to show OEM Logo splash screen first before showing any option ROM text
- Fixed display of cache for multi-core processors.
- Added F10 Save and Exit key functionality to the Intel(R) ME Setup page.
- Fixed the problem where installing Admin/User passwords in Setup hanged the system.
- Modified that user no longer force to change password when switching Manageability Feature from None/ASF to Intel(R) AMT.
- Added error checking to prevent Small-Medium-Business mode always stay in "InProgress" state.

- Fixed an issue where the DRAM Read to Write Delay timing was incorrect for Synchronous/Asynchronous.
- Fixed PID/PPS setup option where not hidden after USB AMT provisioning.
- Fixed EIT changing Video mode when in manufacturing mode.
- Fixed abrupt system restart after F10 Save & Exit in BIOS maintenance mode.
- Simplified setup text for Turn on Intel(R) ME in Sleep States option.
- Allow booting of Non-LVMM devices after LVMM has been installed.
- Changed VT default to disabled.
- Set LT to disabled by default in setup.
- Fixed an issue where the PlatformCpuInfo memory area is not cleared correctly.
- Added support for Windows* Vista Media Center OCUR Host Firmware Support.
- Fixed the issue where some ICH temperature sensor is not updating temperature.
- Added support for disabling the High Definition Codec.
- Fixed issue where local hard disks are not visible from DOS during IDER boot session.
- Fixed a problem where the FERR# multiplexing, IPPrefetcherEnable, and DCUPrefetcherEnable was not set correct on the CPU threads.
- Fixed failures with the TCG ACPI Event Log when running the Vista* DTM TCG TPM BIOS Interface Test.
- Added AMT 2.1 EIT.
- Added MEOnInHostSleepState support for Sx states via Setup for ME Alpha 1 3.0.0.1034 kit.
- Updated SMBIOS Info Type for to compliant with SMBIOS Spec 2.5.
- Added SMBIOS definition for certain processors.

BIOS Version 5718

About This Release:

- January 25, 2006
- CO96510J.86A.5718.2007.0125.1615
- VBIOS info: Build Number: 1402 PC 14.21 11/30/2006 12:21:54.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.0.1028 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Fixed an issue of not saving AMT changes when "Save and Exit" is done through menu.
- Updated the flash descriptor.
- Added support for Winbond* W25X16 16Mb SPI part for ICH8.
- Added support for Windows* Vista* Media Center OCUR Host Firmware Support.

- Fixed Intel(R) Embedded IT Configuration setup option unable to lock or gray out.
- ME Interface fixes.
- Fixed Iflash failure with Winbond SPI flash part.
- Fixed issue where system hangs when trying to load bootable CD from a USB CD drive.
- Added F10 Save and Exit key functionality to the Intel(R) ME Setup page.
- Updated Chassis Type SMBIOS structure.
- Fixed issue where local hard disks are not visible from DOS during IDER boot session.
- Added a fan redetection feature to warn about potential failing fans and disable not working fans.
- Updated Video BIOS Build Number: 1402 PC 14.21 11/30/2006 12:21:54.

BIOS Version 5595

About This Release:

- December 27, 2006
- CO96510J.86A.5595.2006.1227.1649
- VBIOS info: Build Number: 1393 PC 14.21 11/10/2006 17:34:15.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.0.1028 production signed.

Note:
If you have BIOS version 5564 installed, iFlash updates to version 5595 or later may fail. If this happens, you will need to use the BIOS Recovery method to update to BIOS version 5595 or later. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Reverted ME firmware back to version 2.1.0.1028.

BIOS Version 5585

About This Release:

- December 15, 2006
- CO96510J.86A.5585.2006.1215.1058
- VBIOS info: Build Number: 1393 PC 14.21 11/10/2006 17:34:15.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.1.2.1029

Note:
BIOS version 5585 for Intel® Desktop Boards DQ965WC, DQ965GF and DQ965CO adds enhancements to Intel® Active Management Technology. If you have updated your system to BIOS version 5585 or later, the only way to 'back-rev' to a BIOS earlier than 5585 is through the BIOS Recovery method. Details on performing a BIOS Recovery are found at http://support.intel.com/support/motherboards/desktop/sb/CS-023360.htm.

New Fixes/Features:

- Added blocking and warning message display for unsupported processors.
- Reverted to RAID option ROM v6.1.0.1002.
- Fixed failures with the TCG ACPI Event Log when running the DTM TCG TPM BIOS Interface Test.
- Fixed ACPI failures when running the DTM TCG TPM Integration Test.
- Fixed issue where USB CD-ROM drives did not work with BIOS support of AMT 2.0 USB mass storage device provisioning.
- Added Force LAN Disable option that is only visible in ITK & Epcsutil.
- Updated Video BIOS Build Number: 1393 PC 14.21 11/10/2006 17:34:15.
- Added capability to disable CMP.
- Fixed Iflash hang during EBU and reboot flash update.
- Fix for ME wake events when ME is in Moff mode.
- Update to ME 2.1.2.1029.
- Changed VT default to disabled.
- Fixed the display of negative value on BIOS setup Hardware Monitoring Page with some CPUs.
- Added Fan Control support for certain processors.
- Fixed AMT system unable to Iflash when AMT is disabled.
- Fixed issue where BIOS Setup defaults would overwrite current user settings when entering Maintenance Mode.
- Added support for generating event log error message and POST display error message if the board AA# has not been programmed on the board.
- Added support for flash update when using an X64 BIOS build.
- Workaround for GPE generated by GETSEC instruction.
- Enable to build the tree with EFI_DEBUG enabled.
- Disable and hide iQRT setup question on some SKUs.
- Fixed a problem where the memory information in setup was not displayed.
- Fixed the issue where audio disappears after system standby.
- Adjusted the BIOS setup Hardware Monitoring Page output display location.
- Added EPS store of PID and PPS when a save and commit is done.
- Fixed a problem where USB legacy and other SMIs could be turned off by an application, causing system instability.
- Allow booting of Non-LVMM devices after LVMM has been installed.
- Added feature to modify BIOS ID (hour and minute) through OEM JPEG logo.
- Added Mebx EIT Virtual Appliance boot support.
- Added support for Windows Vista SLP 2.0 for standard product (86A) Intel Desktop Board BIOS.
- Boot from USB or other non-EIT drives (after LVMM has been installed) only allowed if admin password installed and entered.
- Added EPS store of PID and PPS.

Known Errata:

- Only Recovery updates are supported when updating this BIOS to a BIOS older than CO5531.
- Recommend Install/Uninstall Virtual Appliance with boot policy set to Normal.

- Use "Save and Commit Settings" for EIT setup changes.
- Remote startup commands may hang system if ME is in m-off state due to expiration of Idle timeout set in ME configuration page.
- Must use BIOS recovery to go back to a previous BIOS (due to the inclusion of iAMT 2.1.

BIOS Version 5493

About This Release:

- November 02, 2006
- CO96510J.86A.5493.2006.1102.1728
- VBIOS info: Build Number: 1377 PC 14.18 09/25/2006 08:09:45.
- SATA RAID info: Intel(R) RAID for SATA - v6.2.0.2002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42

New Fixes/Features:

- Fixed AMT system only able to provision when USB device is present.
- Fixed an issue where auto-recovery from a corrupt image wasn't working.
- Updated SMBIOS Info Type for to compliant with SMBIOS Spec 2.5.
- Fixed issue where user lost control of setup browser if the setup page shows only text.
- Updated CMOS Check summing method.
- IRQ fix for USB Interrupts that conflict with other devices.
- Fixed an issue where pressing ESC key and answering NO will cause the highlight for the selected option to disappear.
- Intel(R) RAID for SATA - v6.2.0.2002.
- Fixed issue where operating system would not enable DMA transfers for SATA drives connected to the ICH.
- Added AMT2.0 Un-provisioning options in Intel(R) ME Setup page.
- Fixed EndOfPost Heci message only being sent when USB device was connected.
- Code clean up for easier support of multiple chipsets.
- Fixed a problem where the system would hang in POST at (13h) if the CPU only supported LT but not VT.
- Fixed issue where BitLocker System Check would not pass.
- Changed AMT 2.0 ACPI SPCR table to only be present when a remote AMT SOL request is made.
- Workaround for GPE generated by GETSEC instruction. Once in every ~1500 power cycles, the processor would generate a general protection exception on the GETSEC instruction. The theory is GPE was generated because the machine check status registers had an error when GETSEC was executed. This workaround is to clear the machine check status registers before GETSEC.
- Implemented support for Hardware-based Watchdog Timer.
- Optimized BIOS boot time.
- Fixed issue where attempting to use the One Time Boot Menu appeared to hang POST.
- Fixed issue where POST errors may be displayed during Maintenance Mode boot.
- Changed to always display the latest event's date and time of event log.
- Fixed an issue where auto-recovery from a corrupt image wasn't working.

- Adding support for Intel® Trusted Execution Technology.
- Fixed a problem where Setup froze when all menu items were grayed out.
- Fixed F10 boot menu showing two lines of duplicated title.
- Fixed Boot Menu title showing "Boot Boot" due to Setup Browser printing the title twice at different rows.
- Moved the multiple TCO Timer implementations in PEI into a single PPI.
- Added support for ACPI Serial Port Console Redirection (SPCR) table for AMT 2.0 SOL.
- Workaround an issue where system intermittently not able to shutdown to S5 if the LAN cable is connected.
- Fixed issue where a carriage return was required at the end of every DSC file
- Removed port 80h debug codes from the memory detection.
- Fixed a problem where the PCI configuration reads to extended PCI configuration space using INT1A functions did not work as expected.
- Fixed an issue where CPU Only Reset PPI does not work.

BIOS Version 5434

About This Release:

- October 16, 2006
- CO96510J.86A.5434.2006.1016.1710
- VBIOS info: Build Number: 1377 PC 14.18 09/25/2006 08:09:45.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.0.5.1124 production signed.

New Fixes/Features:

- Added USB Key Provisioning.
- Added support for ACPI Serial Port Console Redirection (SPCR) table for AMT 2.0 SOL.
- Supports OEM Activation 2.0. For details on the OEM Activation Program, send email to oasignh@microsoft.com
- Hide USB2.0 option in Bios setup menu but show in maintenance mode.
- IRQ Fix for USB Interrupts.
- Updated tables for ASF AMT PET messages.
- Added programming of PCI Subsystem Vendor ID and Subsystem ID for the PCIe Graphics bridge.
- Fix for ITK where Parallel Port is always hidden.
- Video BIOS Build Number: 1377 PC 14.18 09/25/2006 08:09:45.
- Added additional help text message for LT enable/disable question in BIOS setup.
- Fixed several issues for burn-in mode support.
- Fixed an issue where system not able to shutdown to S5 if the LAN is set to D3 mode.
- Fixed an issue where system not able to restart if the LAN is set to D3 mode.
- Skipped LAN initializations during S3 resume.
- Fixed an issue where WOL not working if an AMT system is in non-AMT mode.

BIOS Version 5356

About This Release:

- October 04, 2006
- CO96510J.86A.5356.2006.1004.1611
- VBIOS info: Build Number: 1371 PC 14.18 08/11/2006 17:22:22.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 09-13-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.42
- ME firmware build: 2.0.5.1124 production signed.

New Fixes/Features:

- Added a warning message that selecting AHCI will only work in the Windows Vista OS.
- Added IDCC support for Silego CK505
- Added Performance Memory Profile support.
- Added S5 Wake from RTC Alarm.
- Added support for Generic CK505 clock.
- Added support to allow Flash update as per RCO Flash permission & provisioning detection.
- AMT: Fixed Computer Name setting will not accept '-' as an acceptable character.
- AMT: Web GUI shows blank info for Processor socket field.
- AMT-M1-Power Button Override Fixes.
- BIOS boot time optimizations.
- Changed flash update to not require RCO Flash permission when system is provisioned in Small Business Mode.
- Fix issue where a device behind multiple bridges (2+) will get an invalid IRQ assignment.
- Fixed a missing highlight cursor problem in Setup after pressing F10 and no response.
- Fixed a problem where Legacy Free motherboard hangs after shut down when WOL from S5 option is set to "Stay Off".
- Fixed a problem where Setup F9 key caused unexpected page movement at submenu option.
- Fixed an issue of corrupted splash screen when RAID or AHCI is selected.
- Fixed an issue where iAMT_EN bit (byte 0 bit 4) of CK505 clock not set before ME init.
- Fixed an issue where S3 resume did not work with dual core processors.
- Fixed an issue where system not able to shutdown to S5 if the LAN is set to D3 mode.
- Fixed an issue where the Hard Disk detect code would wait for a 50 seconds on the first boot after a ROM burn.
- Fixed an unexpected system shut down problem after AC Loss.
- Fixed issue where certain security software unable to run properly.
- Fixed F10 boot menu showing two lines of duplicated title.
- Fixed Iflash unable to flash update below 1079 ME Build Number.
- Fixed intermittent Post Code E9 failure during power cycling.
- Fixed issue where changing certain Setup Options and using F10 to Save and Exit would not cause a system reset.
- Fixed issue where disk partitions are sometimes not seen during operating system installation.

- Fixed LAN enable/disable issues by implementing ME global reset if LAN setting changed per ICH8 BIOS spec Rev. 1.0 section 10.3.
- Fixed long flashing time on "/nr" command with certain processor.
- Fixed Removable Devices not showing up in AMT Web UI.
- Fixed Setup cosmetic issue where garbage characters are printed outside of string input box.
- Fixed SMBIOS Type0, Type8, Type9 structures.
- Fixed system continues to boot to next bootable device when no IDER media present during AMT IDER & SOL session.
- Hide SATA Port strings when RAID mode selected.
- New PXE code: Intel(R) Boot Agent GE v1.2.42.
- New Rev of AHCI OROM. This a new AHCI Option ROM based off rev# 1.08 build 09072006.
- Removed redundant SDRAM references from Memory Configuration page in Setup.
- Removed USB 2.0 Enable/Disable question from setup.
- Unhide "HPET Enable/Disable" BIOS setup option and set default state to "Disable".
- Updated AMT ME Firmware to version 1125.
- Updating AFSC configuration files.
- Workaround for issue where Silego CK505 clock not allow single byte write to Byte 12.
- Workaround Silego CK505 clock part glitch when switching spread spectrum (SSC) mode.

BIOS Version 4861

About This Release:

- September 05, 2006
- CO96510J.86A.4861.2006.0905.1540 VBIOS info:
- VBIOS info: Build Number: 1371 PC 14.18 08/11/2006 17:22:22.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 05-08-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.40 Beta-5
- ME firmware build: 2.0.5.1124

New Fixes/Features:

- Changed the code to not reset video mode for every OPROM.
- Added CPU blocking mechanism to block certain processors from running in boards with 3-phase VREG.
- Fixed a problem where Setup didn't show any drive information under Drive configuration menu when a user chose AHCI or Raid mode.
- Modified AMT2.0 Type 130 SMBIOS structure as per ME BWG.
- Fixed a problem where the system would not power down appropriately after a power button press.
- Fixed the issue where we always send AFSC configuration data each boot.
- Fix a problem where the SATA eye-diagram was failing.
- Workaround for AFSC subsystem not getting configured issue.
- Added hard disk SMART error support.
- Fixed a problem where Intel brand badge wasn't displayed when certain processor was installed.
- Hardware-based Watchdog Timer implementation.
- Added support to optionally decode the dash number in the board ID to select a feature mapping.

- AMT: RCO power-off fix Implemented handling of End Of Dram Init Heci message Response details which provide state for system to be in after an RCO power-off operation.
- Removed the Front panel high definition audio setup option for the legacy free boards.
- If the system is in manufacturing mode, do not disable TPM INT1A interface if the BIOS SETUP TPM Enabled question is set to "Disabled".
- Added support for PEG x1 video card to work together with Internal Graphics Device (IGD) to support multi-monitors.
- Added Set PRTC setup option and sync-up AmtBx to Ver 1.1.8.
- Added Setup Option "CPU Fan Speed" for certain CPU Hardware Monitoring configurations.
- Add Heceta6P chip support. Enable PECI feature in certain processors.
- Fixed a problem where the system did not wake up from PING if the network card was inserted in the PEG slot (off the MCH).
- Fixed SMBIOS Type0, Type8, Type9 structures.

BIOS Version 4713

About This Release:

- August 28, 2006
- CO96510J.86A.4713.2006.0828.1752
- VBIOS info: Build Number: 1371 PC 14.18 08/11/2006 17:22:22.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 05-08-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.40 Beta-5

New Fixes/Features:

- Added feature that supports dual monitor between IGD and x1 PEG card for systems that do not have onboard DVI connector.
- Added LT support

BIOS Version 4673

About This Release:

- August 25, 2006
- CO96510J.86A.4673.2006.0825.1113
- VBIOS info: Build Number: 1371 PC 14.18 08/11/2006 17:22:22.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 05-08-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.40 Beta-5

New Fixes/Features:

- iAMT: Added support for RCO "Configuration Data Reset" option when booting in SOL mode.
- iAMT: Support RCO command to Lock Keyboard in BIOS Setup when using SOL.
- iAMT: Added Remote Force HDD boot capability.
- iAMT: Force Always Enable LAN when running in ASF or iAMT manageability mode.
- Fixed Green Bar glitch at DOS boot when SOL is enabled.
- Fixed SMBIOS Type0, Type8, Type9 structures.
- iAMT: Fixed web interface 'Disk' view not showing correct disk size.

- iAMT: Fixed Password required to be redundantly changed when not in iAMT mode.
- Fixed issue where Setup incorrectly displayed processor frequency as 3.6GHz instead of 3.06GHz.
- Fixed issue where USB keyboard was sometimes not functional in BIOS SETUP if attached USB mouse is moved during BIOS SETUP.
- Fixed Setup Time field corruption with SOL.
- Changed HECI failure event message.
- Added support to allow Flash update as per RCO Flash permission & provisioning detection.
- Fixed no BIOS SETUP text in Hyperterminal after first remote iAMT SOL request to enter BIOS SETUP.
- Fixed delay seen when booting to iAMT 2.0 IDER devices.
- Fixed issue where operating system could not initialize TPM 1.2 for BitLocker support.
- Add workaround to reset if write to clock hangs On systems with the Silego clock.
- Fixed the issue where AFSC configuration is not updated after BIOS update.
- Fixed the issue where AFSC always enable all FanTach during each boot.
- Workaround for AFSC subsystem not getting configured issue.
- Added RCO flash permissions, provisioning detection, and global reset after recovery.
- Workaround issue where PCI slot clock not turned on if system not gone through AC cycling.
- Added workaround for Silego CK505 Clock to address issue where certain FSB Overrides would not properly latch.
- Added code to make sure clock is not in full reset mode before doing any setting.
- Fixed an issue where Rev D and newer clock part is not detected correctly.
- Added ability to update ME image through EBU.
- Fixed the issue where Boot Menu will not display correctly after F9 Load Default under certain scenarios.
- Fixed a potential issue that system not loading normal default after manufacturing mode.
- Fixed issue where system not able to shutdown if wake on LAN is set to stay off in BIOS setup.
- Fixed issue where BIOS not correctly detect type of LAN during LAN init.
- Fixed a problem where the system would boot without video when setup option was set to default video device is PCI and no PCI video card was present.
- Fixed continuous reset issues with unlocked CPUs.
- Workaround issue where system hang at POST code 0x13 if system reset is performed during LAN init at PEI stage 1.
- Fixed a problem where the system did not wake up from PING if the network card was inserted in the PEG slot (off the MCH).
- Fixed a problem where the setup options for floppy, LPT, number of SATA ports, etc. did not display correctly on legacy free boards.
- Added "FSB Latch" Setup Option.
- Skip "The Express BIOS update has completed successfully." dialog box when EBU runs in silent mode.
- Fix to resolve the USB HID keyboard typematic issue.

- Fixed issue where the upper portion of the F000 shadow memory region was being set to Read-Only during POST legacy-free USB initialization.

BIOS Version 4462

About This Release:

- August 4, 2006
- CO96510J.86A.4462.2006.0804.2059
- VBIOS info: Build Number: 1348 PC 14.18 06/22/2006 11:01:34.
- SATA RAID info: Intel(R) RAID for SATA - v6.1.0.1002
- SATA AHCI info: Version UPSD src 05-08-2006
- PXE Nahum info: Intel(R) Boot Agent GE v1.2.40 Beta-5

New Fixes/Features:

- Initial production bios release