D   Statement of Volatility

Z440 Workstation

HP confirms that Intel-based Z440 personal workstation contains DDR RAM volatile memory (memory amount depends on the customer configuration). In addition, the motherboard in the condition originally shipped without subsequent modification or the addition or installation of any applications, features, or functionality, contain the following nonvolatile memory: PCH Real Time Clock (RTC) battery backed-up configuration memory (256 Bytes), Super I/O battery backed-up configuration memory (16 Bytes), masked keyboard ROM (2K Bytes), DIMM Serial Presence Detect (SPD) configuration data (256 Bytes per module, 128 Bytes programmable), TPM module (2.35 kB), and Serial Flash IC for System BIOS (128M Bits).

The volatile memory is cleared by removing power from the system for greater than 30 seconds. The nonvolatile memory on the motherboard is restored by following the steps below:

1.   If TPM Ownership has been taken enter F10 setup.

2.   Navigate to the **Security** tab.

3.   Select **TPM Embedded Security > TPM Clear > Clear**.

4.   Save and exit BIOS.

5.   Press F1 when prompted to accept the clearing of the TPM nonvolatile memory.

6.   Download the latest BIOS for this system and operating system off of the HP website.

7.   Follow the instructions on the website to flash the BIOS. This will clear all settings and passwords related to the BIOS.

8.   Power down the system and remove the AC power cord. The RTC and Super I/O battery backed-up memory is cleared by removing the battery found on the motherboard, allowing the board to sit for greater than 60 seconds, and then replacing the battery.

The DIMM SPD EEPROM is not readily available to the user, however there appear to be tools publicly available to read and write this part. To eliminate the possibility that it could contain sensitive information, remove the DIMMs or use one of these tools.

Z640 Workstation

HP confirms that Intel-based Z640 personal workstation contains DDR RAM volatile memory (memory amount depends on the customer configuration). In addition, the motherboard in the condition originally shipped without subsequent modification or the addition or installation of any applications, features, or functionality, contain the following nonvolatile memory: PCH Real Time Clock (RTC) battery backed-up configuration memory (256 Bytes), Super I/O battery backed-up configuration memory (16 Bytes), masked keyboard ROM (2K Bytes), DIMM Serial Presence Detect (SPD) configuration data (256 Bytes per module, 128 Bytes programmable), TPM module (2.35 kB), and Serial Flash IC for System BIOS (128M Bits).

The volatile memory is cleared by removing power from the system for greater than 30 seconds. The nonvolatile memory on the motherboard is restored by following the steps below:

1.   If TPM Ownership has been taken enter F10 setup.

2.   Navigate to the **Security** tab.

3.   Select **TPM Embedded Security > TPM Clear > Clear**.

4. Save and exit BIOS.

5. Press F1 when prompted to accept the clearing of the TPM nonvolatile memory.

6. Download the latest BIOS for this system and operating system off of the HP website.

7. Follow the instructions on the website to flash the BIOS. This will clear all settings and passwords related to the BIOS.

8. Power down the system and remove the AC power cord. The RTC and Super I/O battery backed-up memory is cleared by removing the battery found on the motherboard, allowing the board to sit for greater than 60 seconds, and then replacing the battery.

The DIMM SPD EEPROM is not readily available to the user, however there appear to be tools publicly available to read and write this part. To eliminate the possibility that it could contain sensitive information, remove the DIMMs or use one of these tools.

Z840 Workstation

HP confirms that Intel-based Z840 personal workstation contains DDR RAM volatile memory (memory amount depends on the customer configuration). In addition, the motherboard in the condition originally shipped without subsequent modification or the addition or installation of any applications, features, or functionality, contain the following nonvolatile memory: PCH Real Time Clock (RTC) battery backed-up configuration memory (256 Bytes), Super I/O battery backed-up configuration memory (16 Bytes), SAS FLASH memory (32Mbits) and an EEPROM (64K Bits), masked keyboard ROM (2K Bytes), secondary LOM Flash (4 Mbits), DIMM Serial Presence Detect (SPD) configuration data (256 Bytes per module, 128 Bytes programmable), TPM module (2.35 kB), and Serial Flash IC for System BIOS (128M Bits).

The volatile memory is cleared by removing power from the system for greater than 30 seconds. The nonvolatile memory on the motherboard is restored by following the steps below:

1. If TPM Ownership has been taken enter F10 setup.

2. Navigate to the **Security** tab.

3. Select **TPM Embedded Security > TPM Clear > Clear**.

4. Save and exit BIOS.

5. Press F1 when prompted to accept the clearing of the TPM nonvolatile memory.

6. Download the latest BIOS for this system and operating system off of the HP website.

7. Follow the instructions on the website to flash the BIOS. This will clear all settings and passwords related to the BIOS.

8. Power down the system and remove the AC power cord. The RTC, Super I/O battery backed-up memory and LSI 2308 SAS controller battery backed memory is cleared by removing the battery found on the motherboard, allowing the board to sit for greater than 60 seconds, and then replacing the battery.

The secondary LOM Flash is inaccessible to the user via any publicly available tools. There are programs used by HP in manufacturing and R&D that allow access, but these are not available outside of HP. The embedded LSI 2308 SAS controller flash ROM can be read, written, and erased via a firmware and BIOS utility SASFLASH.exe available in the latest soft pack release on the HP website. The embedded LSI 2308 SAS controller battery backed memory can be erased following the instructions stated above in step 8. The DIMM SPD EEPROM is not readily available to the user, however there appear to be tools publicly available to read and write this part. To eliminate the possibility that it could contain sensitive information, remove the DIMMs or use one of these tools.