Meeting Compliance Requirements for BIOS protection and resiliency

Modern computers rely on the BIOS to facilitate the hardware to load critical components and initiate firmware. It resides outside of and operates independently from the operating system domain.

Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture.

The National Institute of Standards and Technology (NIST) developed guidelines and specifications that provide a framework for organizations to consider in addressing these risks.

In addition to Lenovo implementing NIST SP800-147 on ThinkPads, ThinkCentres, and ThinkStations, we provide additional distinct security advantages

As cyber-attacks are increasing in frequency against the client devices, Lenovo recognizes the importance of adhering to the NIST guidelines while providing additional security measures:

- While many OEM's implement a functionality in their BIOS which can allow anyone to reset passwords that protect the integrity of the BIOS, Lenovo BIOS does not contain any such ability to reset the master supervisor password
- Lenovo solutions are implemented around industry standard UEFI code minimizing compatibility issues around enabling MSFT L3 security, giving our customers greater resilience against unexpected technical compatibility issues
- We allow customers to visually inspect all Lenovo Think commercial products' BIOS source code in a controlled physical environment. Nearly 2 MILLION lines of source code available for inspection*
- Lenovo's standard image only includes the operating system and related software, software required to make hardware work well (for example, when we include unique hardware in our devices, like a 3D camera, security software and Lenovo applications)

Lenovo has enabled BIOS resiliency on 2019 ThinkPads

Modern computing systems architectures are thought of as layers with the top layers being software, composed of operating system and applications. The underlying layers of the platform includes hardware and firmware components, such as the BIOS:

- ThinkPads detect corruption of all primary BIOS code region and recovers corrupted region if detected by booting from the backup region and recover the corrupted primary region with the binary in the backup region

- ThinkPads will also update the backup region when the primary region is updated with the new processor microcode or vulnerability fix

- Lenovo ThinkPads are embedded with trusted technology:

    - *Intel Boot Guard* prevents the execution of unauthorized Initial Boot Block (IBB) and to detect the corruption of the IBB
    - *Top Swap* switches the IBB region with the alternate region with an external signal and is used to boot from the backup region when primary region is corrupted.
    - Software based BIOS Self-Healing for BIOS backup and restore function powered by *Phoenix*

Lenovo's next generation devices are being developed to ensure the platform's firmware code and critical data are always in a state of integrity

- Lenovo is committed to the NIST SP800-193 standard and will continue to evolve over time

- We will implement an EC based solution that melds the best of both worlds together in the next gen ThinkPad – ThinkCentre will follow

- Additionally, we are working with several partners to provide an advanced solution based on NIST SP800-155