UEFI FORUM ANNOUNCES NEW WHITE PAPER ON THE CHAIN OF TRUST

White paper is the first in a series dedicated to safeguarding the future of computing

Beaverton, Ore.—June 21, 2016—Today, the UEFI Forum announced the availability of a new white paper. "The Chain of Trust: Keeping Computing Systems More Secure" is the first in a series of white papers that explores best practices for locking down the firmware platform using an approach called Chain of Trust (CoT). CoT helps users gain more confidence that their computing system is as safe and free from different classes of attacks as possible.

The new whitepaper can be downloaded here – http://www.uefi.org/learning_center/papers.

"Since its inception, the "Chain of Trust" represents numerous computing industry members' collective vision of greater security from power up to application deployment," says UEFI board member, Richard Wilkins, Ph.D. Phoenix Technologies, Ltd. "Its goal is to give the end user confidence that nothing along the chain can be compromised. The vision is dependent on security measures taken by all players operating at each stack layer…or "link" in the chain—not just at the firmware layer."

Today, firmware security methods vary generally due to usage scenarios, manufacturing demands and developer preferences. The industry call to action is to document and to communicate openly the deployed methods so that developers know what security information is available to them. Developers can then determine what, if any, other steps are required to further secure a system. The series of white papers provides an overview and general guidelines of the CoT approach, security technologies, initiative and deployment best practices. The next white paper in the series is due out in July.

About UEFI Forum

The UEFI Forum, a non-profit industry standards body, champions firmware innovation through industry collaboration and the advocacy of a standardized interface that simplifies and secures platform initialization and firmware bootstrap operations. Both developed and supported by representatives from more than 300 industry-leading technology companies, UEFI Forum specifications promote business and technological efficiency, improve performance and security, facilitate interoperability between devices, platforms and systems, and comply with next-generation technologies.

The Forum's spheres of input and influence are large: Membership represents major voices from all players in the industry—open source to proprietary technology, hardware to software, mobile to stationary devices. The Forum collaborates with other standards groups that are essential to computing. For more information about the UEFI Forum and current specification go to www.uefi.org.

# # #