



National Security Agency
Cybersecurity Technical Report

UEFI Secure Boot Customization

March 2023 ver. 1.2

S/N: U/OO/168873-20
PP-23-0464



Notices and history

Document change history

Date	Version	Description
15 September 2020	1.0	Publication release.
16 September 2020	1.1	Updated server UEFI hash interface image and text.
14 March 2023	1.2	Updated DB and DBX hash calculation information in section 4.3.3 to correctly handle EFI (PE/EFL) format.

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

Trademark recognition

Dell, EMC, Dell EMC, iDRAC, Optiplex, and PowerEdge are registered trademarks of Dell, Inc.

HP, HPE, HP Enterprise, iLO, and ProLiant are registered trademarks of Hewlett-Packard Company.

Linux is a registered trademark of Linus Torvolds.

Microsoft, Hyper-V, Surface, and Windows are registered trademarks of Microsoft Corporation.

Red Hat, Red Hat Enterprise Linux (RHEL), CentOS, and Fedora are registered trademarks of Red Hat, Inc.

VMware and ESXI are registered trademarks of VMware, Inc.

Trusted Computing Group, TCG, Trusted Platform Module, TPM, and related specifications are property of the Trusted Computing Group.

Unified Extensible Firmware Interface, UEFI, UEFI Forum, and related specifications are property of the UEFI Forum.



Publication information

Author(s)

National Security Agency
Cybersecurity Directorate
Endpoint Security Division
Platform Security Section

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Additional resources

Please visit the NSA Cybersecurity GitHub at <https://www.github.com/nsacyber/Hardware-and-Firmware-Security-Guidance> for additional resources relating to UEFI Secure Boot and the customization process.

