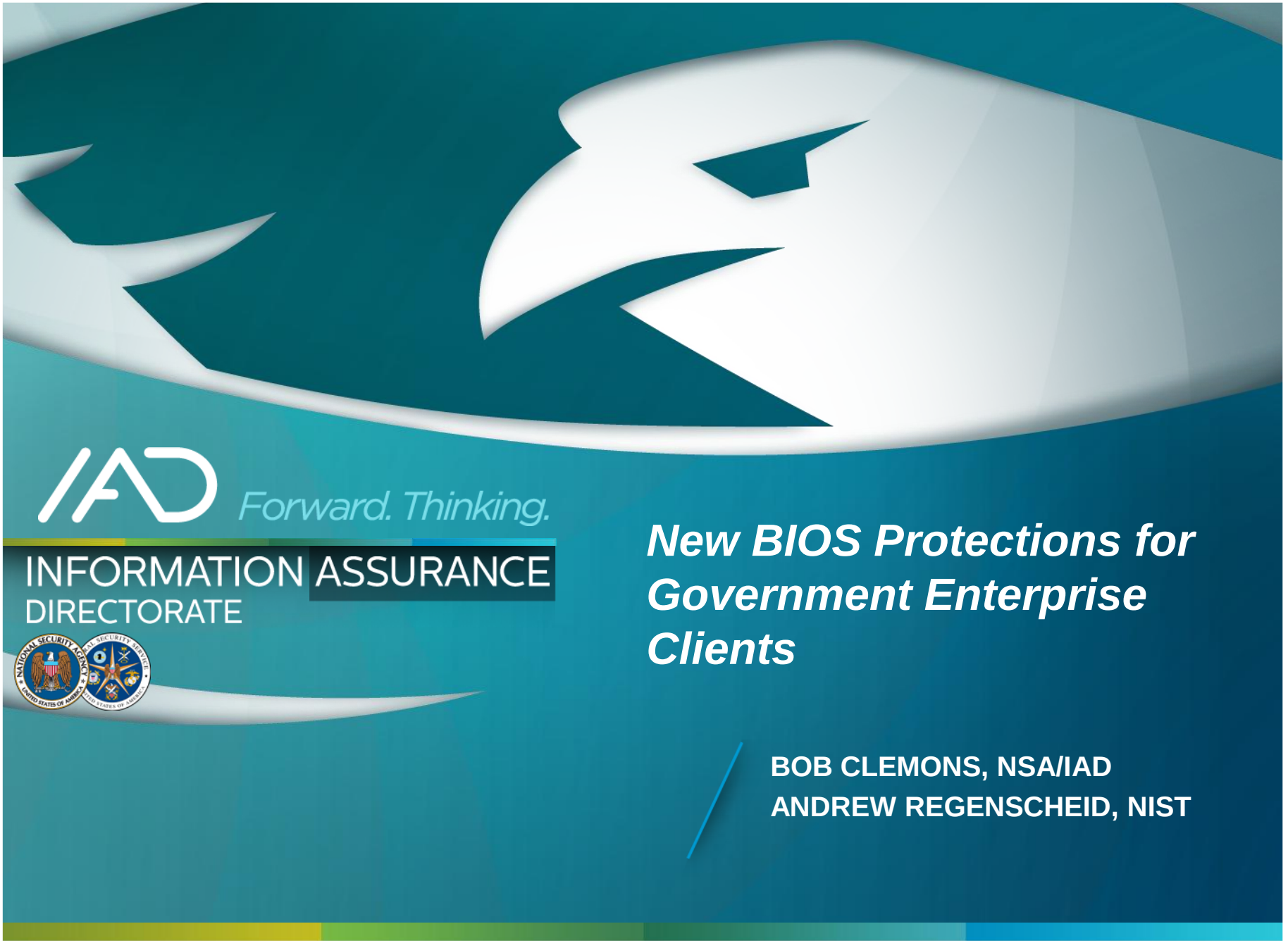


New BIOS Protections for Government Enterprise Clients

BOB CLEMONS, NSA/IAD
ANDREW REGENSCHEID, NIST

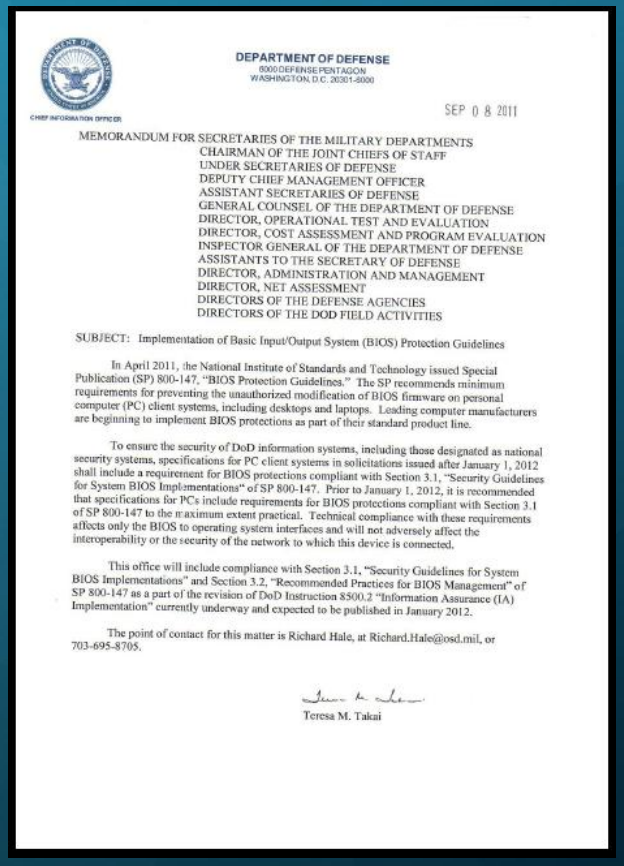
GOALS

- From this talk you should learn:
  - What it means for systems to be compliant with the NIST Special Publications
  - What you gain from running systems compliant with the NIST Special Publications
  - Why you should care

Outline

- Background
- Prevention of Unauthorized BIOS Modification (NIST SP 800-147)
- Detection of Unauthorized BIOS Modification (NIST SP 800-155)
- Recommendations

BIOS PROTECTION MEMORANDA



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

SEP 0 8 2011

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Implementation of Basic Input/Output System (BIOS) Protection Guidelines

In April 2011, the National Institute of Standards and Technology issued Special Publication (SP) 800-147, "BIOS Protection Guidelines." The SP recommends minimum requirements for preventing the unauthorized modification of BIOS firmware on personal computer (PC) client systems, including desktops and laptops. Leading computer manufacturers are beginning to implement BIOS protections as part of their standard product line.

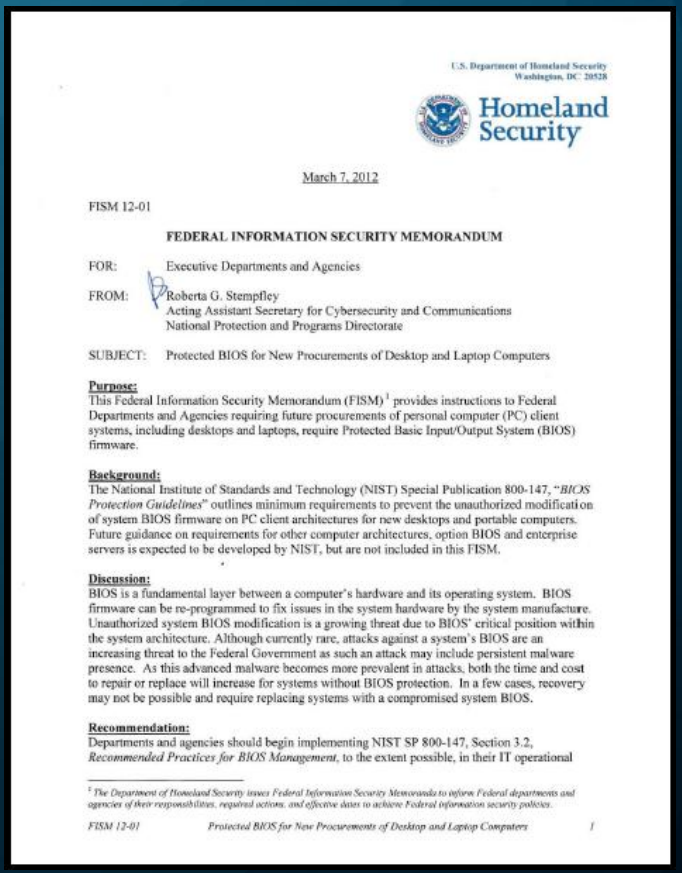
To ensure the security of DoD information systems, including those designated as national security systems, specifications for PC client systems in solicitations issued after January 1, 2012 shall include a requirement for BIOS protections compliant with Section 3.1, "Security Guidelines for System BIOS Implementations" of SP 800-147. Prior to January 1, 2012, it is recommended that specifications for PCs include requirements for BIOS protections compliant with Section 3.1 of SP 800-147 to the maximum extent practical. Technical compliance with these requirements affects only the BIOS to operating system interfaces and will not adversely affect the interoperability or the security of the network to which this device is connected.

This office will include compliance with Section 3.1, "Security Guidelines for System BIOS Implementations" and Section 3.2, "Recommended Practices for BIOS Management" of SP 800-147 as a part of the revision of DoD Instruction 8500.2 "Information Assurance (IA) Implementation" currently underway and expected to be published in January 2012.

The point of contact for this matter is Richard Hale, at Richard.Hale@osd.mil, or 703-695-8705.

Teresa M. Takai

DOD CIO Memo NII001001
8 Sept 2011



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 7, 2012

FISM 12-01

FEDERAL INFORMATION SECURITY MEMORANDUM

FOR: Executive Departments and Agencies

FROM: Roberta G. Stempfley
Acting Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

SUBJECT: Protected BIOS for New Procurements of Desktop and Laptop Computers

Purpose:
This Federal Information Security Memorandum (FISM)[1] provides instructions to Federal Departments and Agencies requiring future procurements of personal computer (PC) client systems, including desktops and laptops, require Protected Basic Input/Output System (BIOS) firmware.

Background:
The National Institute of Standards and Technology (NIST) Special Publication 800-147, "*BIOS Protection Guidelines*" outlines minimum requirements to prevent the unauthorized modification of system BIOS firmware on PC client architectures for new desktops and portable computers. Future guidance on requirements for other computer architectures, option BIOS and enterprise servers is expected to be developed by NIST, but are not included in this FISM.

Discussion:
BIOS is a fundamental layer between a computer's hardware and its operating system. BIOS firmware can be re-programmed to fix issues in the system hardware by the system manufacturer. Unauthorized system BIOS modification is a growing threat due to BIOS' critical position within the system architecture. Although currently rare, attacks against a system's BIOS are an increasing threat to the Federal Government as such an attack may include persistent malware presence. As this advanced malware becomes more prevalent in attacks, both the time and cost to repair or replace will increase for systems without BIOS protection. In a few cases, recovery may not be possible and require replacing systems with a compromised system BIOS.

Recommendation:
Departments and agencies should begin implementing NIST SP 800-147, Section 3.2, *Recommended Practices for BIOS Management*, to the extent possible, in their IT operational

[1] *The Department of Homeland Security issues Federal Information Security Memoranda to inform Federal departments and agencies of their responsibilities, required actions, and effective dates to achieve Federal information security policies.*

DHS FISM 12-01
7 Mar 2012

DOD CIO MEMORANDUM

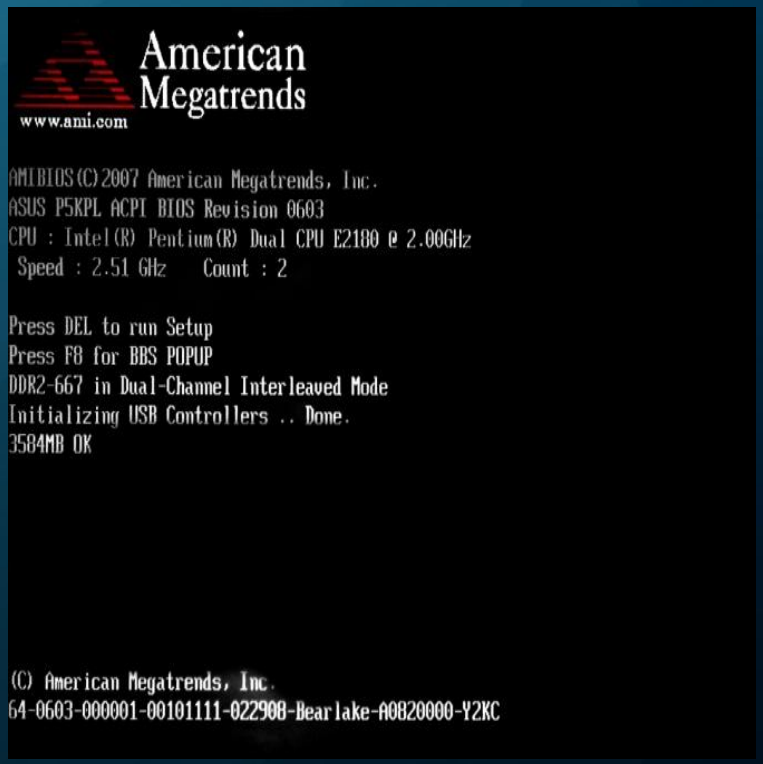
- Applies to DoD Information Systems
- Requires specifications for “PC client systems” in solicitations issued after 1 Jan 2012 to require compliance with NIST Special Publication 800-147 section 3.1
- Compliance with 800-147 sections 3.1 and 3.2 to be included in revised DoD Instruction 8500.2 “Information Assurance (IA) Implementation”

DHS MEMORANDUM

- Applies to Federal Departments and Agencies
- Recommends that new procurements of PC client systems after 1 Oct 2012 be compliant with 800-147 section 3.1 “to the extent possible”
- Permits update through normal refresh cycle
- Recommends implementing 800-147 section 3.2 “to the extent possible”

WHAT IS BIOS?

- Basic Input/Output System
- Firmware that initializes and boots the system
- Stored on motherboard and add-in cards



SYSTEM BIOS

- Stored on flash device on the motherboard
- First code to execute on the main processor after power on
- Two major types of PC BIOS
  - Conventional/Legacy BIOS
  - Unified Extensible Firmware Interface (UEFI)

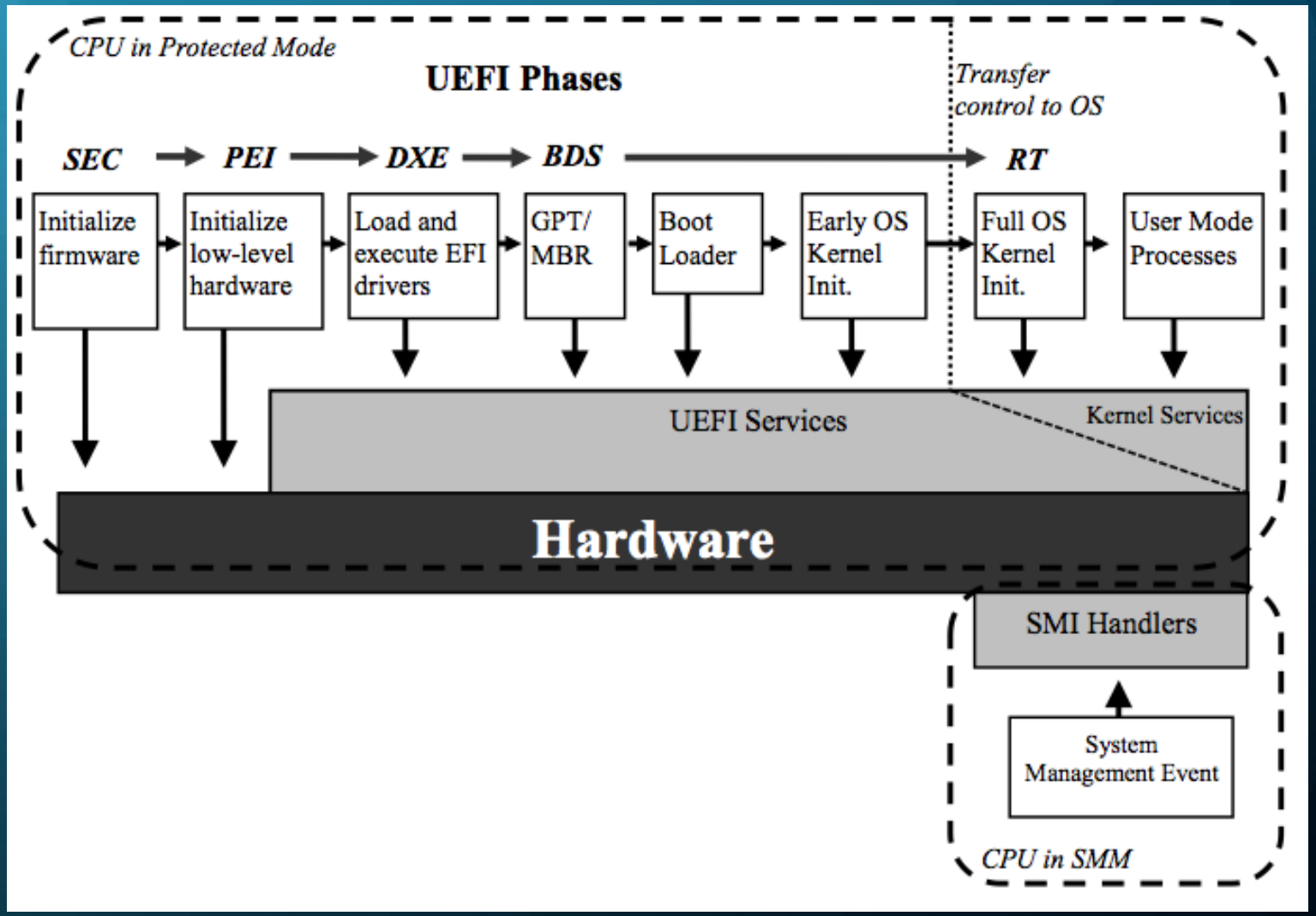
OTHER FIRMWARE

- Option ROMs
  - BIOS code on add-on cards (e.g., video card, HDD controller)
  - Developed and updated by add-on card manufacturer
  - Executes during boot on main CPU
- Microcontroller Firmware
  - Executes on add-on card microcontroller (e.g., HDD, DVD drive, HW management engine)
  - Developed and updated by add-on card manufacturer

PC BOOT PROCESS

- Execute Core Root of Trust
- Initialize and Test Low-Level Hardware
- Load and Execute Additional Firmware Modules
- Select Boot Device
- Load Operating System

UEFI BOOT PROCESS



BIOS UPDATES

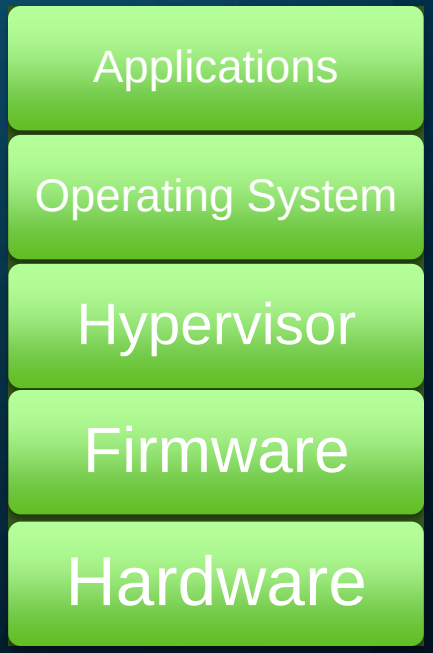
- System BIOS is updatable
  - To patch vulnerabilities
  - To add features
- Update mechanisms
  - User-initiated updates
  - Managed updates
  - Rollback
  - Manual recovery
  - Automatic recovery

THREATS

- Destructive Modification
  - Erase or corrupt the BIOS so the system will not boot
  - Might require physical replacement of BIOS chip
  - e.g., CIH (Chernobyl)
- Persistence Modification
  - A BIOS modification that ensures the continued existence of malware elsewhere
  - e.g., Mebromi
    - Infects BIOS, MBR, OS

MOTIVATION

- Operating system defenses have improved
- Malware has moved from the operating system to applications
- Firmware is another (more privileged) place for malware to go



WHY NOW?

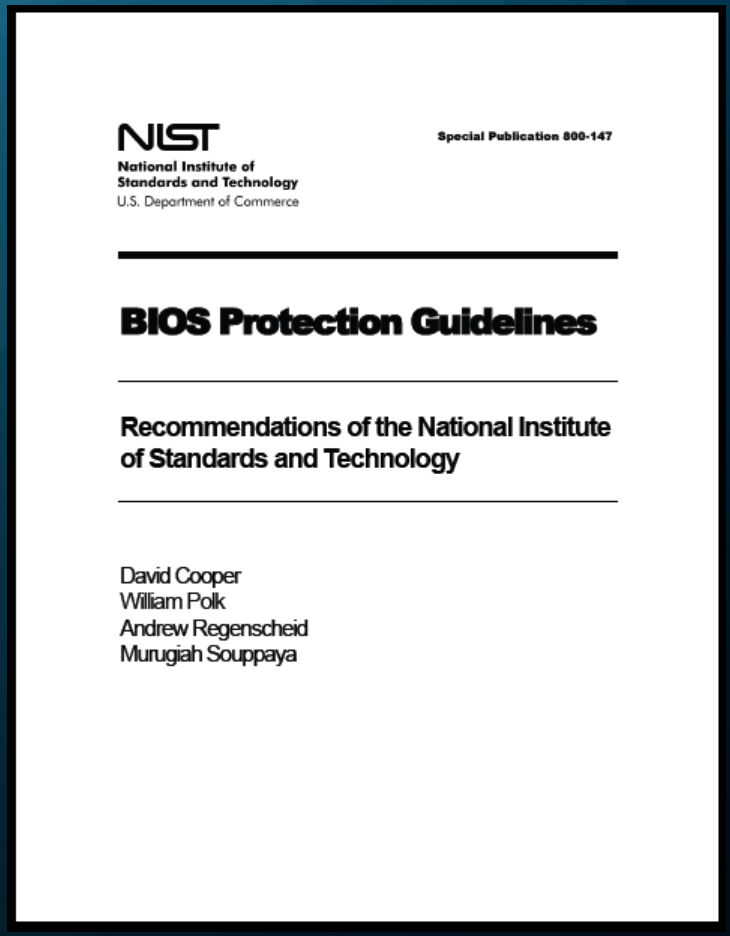
- Computer industry is transitioning to UEFI-based BIOS implementations
- UEFI is very different from conventional BIOS:
  - More security features defined
  - Much larger attack surface
  - Standard interfaces could make exploits easier to write
- NIST had an opportunity to influence products before attacks become widespread

NIST GUIDELINES

- Two-pronged approach
  - **Protect** System BIOS from unauthorized modification by implementing a secure update mechanism (SP 800-147)
  - **Detect** unauthorized modification of System BIOS and configuration using secure measurement and reporting mechanisms (SP 800-155)

NIST SP 800-147
BIOS PROTECTION GUIDELINES

- Scope
  - System BIOS
    - Not option ROMs or microcontroller firmware
  - x86-based desktops and laptops
    - Not servers, tablets, phones
  - Remote threats
    - Malware exploits update mechanism
    - Compromised enterprise management infrastructure
    - Rollback to a vulnerable BIOS



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-147

BIOS Protection Guidelines

Recommendations of the National Institute of Standards and Technology

David Cooper
William Polk
Andrew Regenscheid
Murugiah Souppaya

ORGANIZATION OF 800-147

- Section 3.1
  - *Guidelines on BIOS Implementations*
  - Intended for computer manufacturers
- Section 3.2
  - *Recommended Practices for Managing the BIOS*
  - Intended for system administrators/owners

SECTION 3.1

- *Security Guidelines for System BIOS Implementations*
  - Signed BIOS updates
  - Flash write protections
  - Non-bypassability
  - Does not protect against physical access!
    - Secure Local Update Mechanism (SLUM)
  - Rollback prevention recommended
    - Prevent update to an authentic, but bad BIOS
  - Says nothing about the goodness of the BIOS!

AUTHENTICATION

1. OEM creates update image
2. OEM signs update image with private key
3. OEM releases update package
4. Package executed on target machine
5. RTU on target machine verifies signature
6. Target machine performs update

ROOT OF TRUST FOR UPDATE (RTU)

- Must contain
  - Signature verification algorithm, and
  - Public key to verify update image
- Which must be
  - stored in a protected fashion, and
  - modifiable only through an authenticated update mechanism or secure local update

SIGNED UPDATE

- Use of NIST-approved crypto algorithms
  - Process: NIST SP 800-89
  - Algorithms: NIST FIPS 186-3
  - Strength: NIST SP 800-131A (>112 bits)
- Recovery mechanisms must also comply (or use SLUM)
- Can allow organizational control of update (authorization)

INTEGRITY (WRITE) PROTECTION

- Protect system BIOS in flash from modification outside of authenticated update process
  - Protect RTU
  - Protect locking mechanism itself
- Invoke protections prior to executing code that is not covered by the authenticated update mechanism
- Recommends hardware protections
  - Chipset-based locks
  - Flash-part-based locks

NON-BYPASSABILITY

- All BIOS updates must go through the authenticated update mechanism
- System design should not permit bypass of BIOS protections, e.g.,
  - No Direct Memory Access to system flash by other hardware components
  - No vulnerabilities in BIOS code
  - No insecure flash locking mechanisms

COMPLIANCE

- Currently self-certifying
- Windows Hardware Certification Requirements
  - "*Further, it is recommended that manufacturers writing BIOS code adhere to the NIST guidelines set out in NIST SP 800-147*"
    - section System.Fundamentals.Firmware.UEFISecureBoot .8

SECTION 3.2

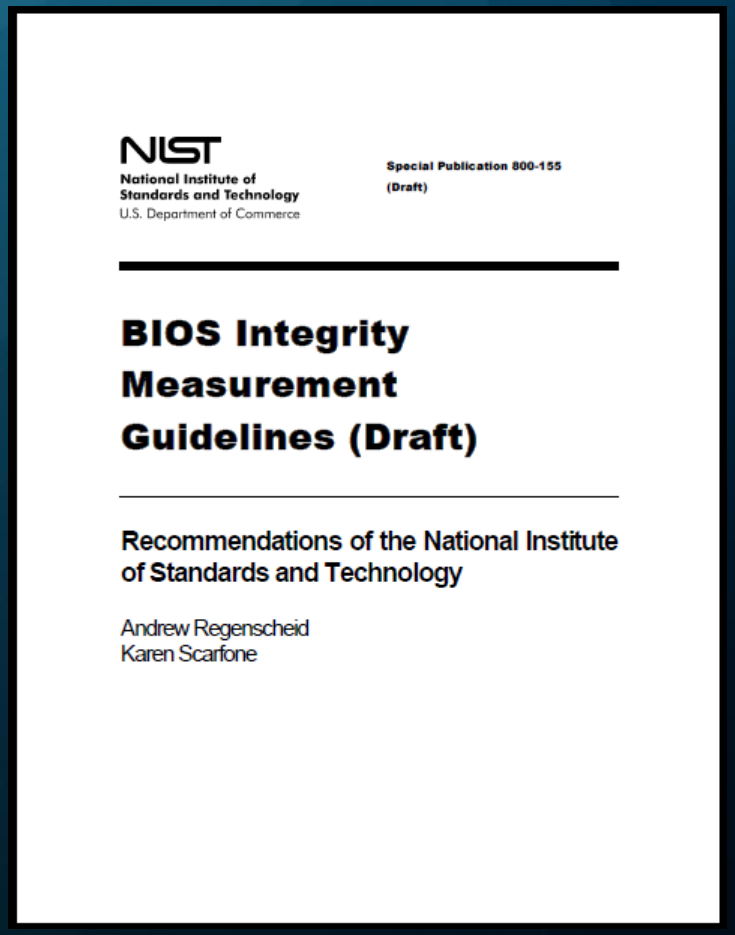
- *Recommended Practices for BIOS Management*
  - Keep track of deployed versions
  - Use the authenticated update mechanism to update BIOS
  - Monitor the BIOS for deviations and remedy if necessary

BONUS RECOMMENDATIONS

- If your systems do not already have 800-147-compliant BIOSes, then you should update if compliant BIOSes are available for your systems
- BIOS Update Guidance

NIST SP 800-155
BIOS INTEGRITY MEASUREMENT GUIDELINES

- Detecting unauthorized changes to BIOS using secure integrity measurement and reporting
- Because protection might not be sufficient
  - Vulnerabilities in authenticated update mechanism could allow malicious update
  - Sensitive configuration data might not be protected
- Guidelines for OEMs, OS vendors, security software vendors, and IT infrastructure manufacturers


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-155
(Draft)

BIOS Integrity Measurement Guidelines (Draft)

Recommendations of the National Institute of Standards and Technology

Andrew Regenscheid
Karen Scarfone

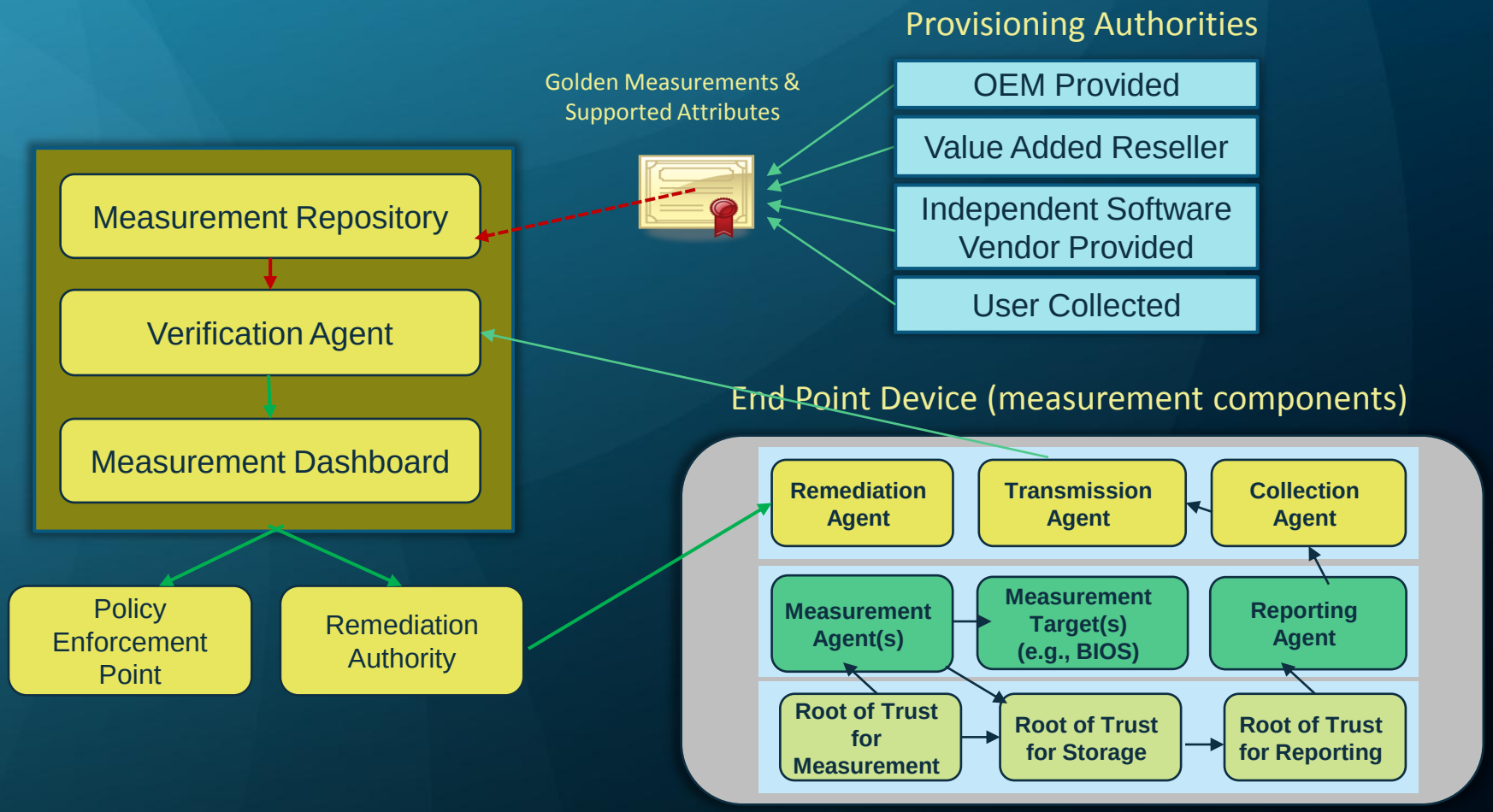
BIOS MEASUREMENT

- Goal: Detect unauthorized changes so administrators can remedy
- Means:
  - Roots of Trust to measure, store, and report to Measurement Assessment Authority (MAA)
  - MAA verifies measurements
  - MAA can instruct IT components (e.g., managed switch) to respond accordingly

CORE COMPONENTS

- Roots of Trust
  - Measurement: Hashes code and data
  - Storage: Secure storage of hashes
  - Reporting: Provides integrity and non-repudiation for measurement reports
- Software agents
  - Untrusted software that interacts with the roots of trust

INTEGRITY MEASUREMENT ARCHITECTURE



MEASUREMENT FLOW

- Device Provisioning
  - Obtain initial measurements from vendor or generate during provisioning
- Measurement
  - BIOS code and configuration data measured by RTM (or chain rooted in RTM) during boot
  - Measurements protected by RTS

MEASUREMENT FLOW

- Reporting
  - MAA receives measurements from endpoint periodically or on request
  - CA and RA use RTR to generate signed report
  - TA sends report to MAA
- MAA Verification
  - Verify signature and measurements
  - Measurements stored for administrators or used for access control decisions

ATTRIBUTES AND MEASUREMENTS

- Attributes
  - Defined properties of a system that are used to assess confidence in the system and its measurements
    (e.g., types of roots of trust, support for 800-147)
- Measurements
  - Cryptographic hashes of code and/or data
- Measurement Logs
  - Measurements and components measured
- Integrity Measurement Registers
  - Protected locations where hashes of measurements are stored

USES CASES

- Basic Measurements Reporting
  - Notify administrators of changes
- Comply-to-Connect
  - Network access control
  - TNC framework
- Continuous Monitoring

RECOMMENDATIONS

- New computer purchases should include an 800-147-compliant BIOS
  - Immediate security benefit
  - Becoming standard
- Update to 800-147-compliant BIOSes if available
  - If not available, consider the criticality of the unprotected systems
- New computer and IT infrastructure purchases should support BIOS measurement
- Make BIOS management part of platform lifecycle

PLATFORM LIFECYCLE

- Provisioning
- Platform Deployment
- Operations and Maintenance
- Recovery
- Disposition

PROVISIONING AND DEPLOYMENT

- Maintain “golden” BIOS image for each platform
- Create and maintain configuration baseline
- Maintain a copy of the RTU, if applicable
- Register endpoint identity and BIOS integrity information in system inventory

PROVISIONING AND DEPLOYMENT

- Load “golden” BIOS image
- Ensure BIOS is configured according to baseline
- Set BIOS password
- Assert security controls requiring physical presence

OPERATION AND MAINTENANCE

- Perform updates using a change management process
  - Use 800-147 authenticated update mechanism
  - BIOS updates require new measurements to be registered
  - Ensure proper configuration is maintained
- Monitor deployed BIOSes

RECOVERY

- Use only when authenticated updates are not possible
- Can be used to rollback from a buggy BIOS update

DISPOSITION

- Reset BIOS configuration to defaults
- Remove passwords and organization-specific cryptographic keys
- Remove organization-specific customizations

SUMMARY

- NIST SP 800-147
  - Protects desktop & laptop clients from unauthorized BIOS modification by defining a secure, non-bypassable authenticated update mechanism
- NIST SP 800-155
  - Outlines a framework for a secure BIOS integrity measurement and reporting chain for client systems

RECENT / FUTURE DEVELOPMENTS

- Additional Protection Guidelines
- Additional Integrity Measurement Guidelines

MORE INFORMATION

NIST BIOS Security publications
available at:
csrc.nist.gov

Contact Information

Andrew Regenscheid
andrew.regenscheid@nist.gov