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 manufacture. 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.*

environment for PC client systems, including desktops and laptops. By October 1, 2012, departments and agencies should include the requirement for BIOS protections compliant with NIST SP 800-147, Section 3.1, *Security Guidelines of System BIOS Implementation*, to the extent possible, in new procurements of PC client systems, including desktops and laptops. Agencies may continue to use existing procurement vehicles, desktops and laptops until updated as part of the agency's normal technology refresh cycle. Several computer manufactures include protected BIOS as a standard option in their enterprise PC lines.

Authorities:

- Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541-3549
- Office of Management and Budget's (OMB) M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and DHS*, 2010
- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, *Comprehensive National Cybersecurity Initiative,* 2009
- Reference: NIST Special Publication 800-147, "*BIOS Protection Guidelines*," (http://csrc.nist.gov/publications/PubsSPs.html)

Additional Information and Contacts:

- Please direct questions regarding this FISM to Sean Donelan, Federal Network Security Branch, Department of Homeland Security FNS.NIS@DHS.gov or (703) 235-5122.