STATE OF ALABAMA

Information Technology Guideline

GUIDELINE 662G2-00: BIOS PROTECTION

A computer's BIOS (Basic Input/Output System) facilitates the hardware initialization process and the startup of the operating system when the computer is powered on; it supplies the first instructions to the computer's microprocessor. Because of its unique and privileged position within the PC architecture, the unauthorized modification of BIOS firmware by malicious software constitutes a significant threat.

OBJECTIVE:

Provide guidelines for preventing unauthorized modification of system BIOS.

SCOPE:

The guidelines in this document apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

GUIDELINES:

The following considerations for managing system BIOS in an enterprise operational environment are based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-147: BIOS Protection Guidelines.

BIOS UPDATE PROCESSES

AUTHENTICATED UPDATE PROCESS:

The authenticated BIOS update process employs digital signatures to ensure the authenticity of the BIOS update image. To update the BIOS using the authenticated update process, there must be a Root of Trust for Update (RTU) that contains a signature verification algorithm and a key store that includes the public key needed to verify the signature on the BIOS update image. Authentication verifies that a BIOS update image was generated by an authentic source and is unaltered.

SECURE LOCAL UPDATE PROCESS:

The secure local update process provides a means of updating the system BIOS without using the authenticated update process. A secure local update should ensure the authenticity and integrity of the BIOS update image by requiring physical presence. Further protections may be implemented in the secure local update process by requiring the entry of an administrator password or the unlocking of a physical lock (e.g., a motherboard jumper) before permitting the system BIOS to be updated. The secure local update process, if it is implemented, should be used only to load the first BIOS image or to recover from a corruption of a system BIOS that cannot be fixed using the authenticated update process.

RECOMMENDED PRACTICES FOR BIOS MANAGEMENT

Recommended practices for BIOS management focus on key activities revolving around provisioning, deploying, managing, and decommissioning the system BIOS as part of its overall platform life cycle.

PROVISIONING PHASE:

Configuration Control:

Institute a mechanism for identifying, inventorying, and tracking the different computer systems across the enterprise throughout their life cycle.

Identify and monitor the BIOS image characteristics such as manufacturer name, version, or time stamp (allows the organization to perform update, rollback, and recovery).

Maintain a "golden master image" for each approved system BIOS, including superseded versions, in secure offline storage.

Create a common configuration baseline for each platform. The baseline should ensure that the integrity protection and non-bypassability features are enabled (if they are configurable), and organization policies for password policy and device boot order are enforced. The BIOS image information and associated baseline of settings for each platform should be documented (e.g., in a configuration management plan).

Key Storage:

If the platform has a configurable Root of Trust for Update (RTU), the organization needs to maintain a copy of the key store and signature verification algorithm. If the RTU is integrated into the system BIOS then this is satisfied by maintaining the golden BIOS image. If the RTU is not integrated into the system BIOS, the security afforded the RTU should be at least as strong as that for the golden BIOS image.

Most organizations will rely upon the manufacturer as the source for the authenticated BIOS. In this case, the organization does not maintain any private keys, and the RTU contains only public keys provided by the manufacturer.

Where the organization prefers to participate actively in the BIOS authentication process by countersigning some or all approved system BIOS updates, the RTU may contain one or more public keys associated with the organization. In this case, the organization must securely maintain the corresponding private key so that the next BIOS update can be signed. Private keys should be maintained under multi-party control to protect against insider attacks. For organizational keys, the corresponding public keys must also be maintained securely (to ensure authentication of origin).

PLATFORM DEPLOYMENT PHASE:

The secure local update process should be used to provision the approved BIOS for that platform from the golden master image, the corresponding RTU should be installed, and BIOS-related configuration parameters established before computer systems are deployed. This will help the organization maintain a consistent, known starting posture.

The organization should periodically perform assessments to confirm that the organization's BIOS policies, processes, and procedures are being followed properly.

OPERATION AND MAINTENANCE PHASE:

This phase includes the activities that are important for maintaining BIOS security and reliability in the operational environment.

System BIOS updates should be performed using a structured change management process (Note: State IT Policy 605 requires that organizations implement a configuration management process).

The new approved version should be documented in the configuration plan, noting the previous BIOS image has been superseded.

The BIOS image and configuration baseline should be continuously monitored. If an unapproved deviation from this baseline is detected, the event should be investigated, documented, and

remediated as part of incident response activities. The secure local update process should be used to recover from a BIOS image compromise (see Handling Exceptional Conditions; next page).

When a new BIOS image is required to extend system capabilities, improve system reliability, or remediate software vulnerabilities, BIOS updates should be performed using the authenticated update process. Where the organization participates actively in the update process, a multi-party control process should be executed to retrieve the private key from secure storage and generate the digital signature. The BIOS installation package should also be signed, and the digital signature should be verified before execution. Once the update has executed successfully, the configuration baseline should be validated to confirm that the computer system is still in compliance with the organization's defined policy.

DISPOSITION PHASE:

The activities in this phase of the platform life cycle reduce the chance of accidental data leakage.

Before the computer system is disposed and leaves the organization, the organization should remove or destroy any sensitive data from the system BIOS. The configuration baseline should be reset to the manufacturer's default profile; in particular, sensitive settings such as passwords should be deleted from the system and keys should also be removed from the key store. If the system BIOS includes any organization-specific customizations then a vendor-provided BIOS image should be installed.

HANDLING EXCEPTIONAL CONDITIONS

In some circumstances, a BIOS update will be required that cannot be accomplished using the authenticated update process. For example, a corrupted system BIOS or RTU may be unable to execute or invoke the authentication procedures. In this case, the appropriate system BIOS and/or RTU may be able to be installed using the secure local update process. In other cases, a BIOS update may have unintended consequences, forcing the organization to roll back to an earlier version. Extra steps may be required for an authenticated update to authorize rollback (if versioning or timestamps are compared during the authentication process), or the secure local update process may be required to reestablish a secure baseline.

As with the Operations and Maintenance phase, it is essential to validate the configuration of the BIOS against the organization's defined policy after BIOS rollback or reinstallation.

ADDITIONAL INFORMATION:

Information Technology Policy 662: Systems Security
http://cybersecurity.alabama.gov/documents/Policy_662_Systems_Security.pdf

Information Technology Policy 605: Configuration Management
http://cybersecurity.alabama.gov/documents/Policy_605_Configuration_Management.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
662G2-00	12/14/2011	Original document