Title:	SECURE CONFIGURATION FOR WINDOWS OPERATING SYSTEM		
NOAA IT Standard Number (NISN):	4.001	Current Version Date:	September 4, 2007
Effective Date:	September 4, 2007	Expiration Date:	n/a
Originator:	Enterprise Architecture Committee	Current Editor:	Enterprise Architecture Committee

PURPOSE AND SCOPE

NOAA currently has various operating system (OS) configurations for personal computer desktops and laptops throughout the organization, but lacks an enterprise standard OS configuration. This situation increases the complexity of designing and implementing centralized systems with consistent security policies, and deprives the technology refresh process of a target enterprise OS configuration baseline to guide future acquisitions of personal computer desktops and laptops.

Related to the above, OMB Memorandum M-07-11 (Implementation of Commonly Accepted Security Configurations for Windows Operating Systems) requires agencies with Windows XP and Vista deployed to adopt the standard security configurations developed by the National Institute of Standards (NIST), Department of Defense (DoD) and Department of Homeland Security (DHS) by February 1, 2008. To facilitate implementation and persistence of the standard configuration, OMB Memorandum M-07-18 (Ensuring New Acquisitions Include Common Security Configurations) requires new acquisitions to include contract language regarding the required configurations.

To ensure compliance with these OMB directives and enhance NOAA's capacity to efficiently manage and securely operate its personal computer desktops and laptops, this policy:

a) Establishes the Federal Desktop Core Configuration (FDCC) as the standard OS configuration for all Windows based personal computer desktops and laptops in NOAA. The NOAA Technical Reference Model (TRM) will document the particular version(s) of the Windows OS currently approved for use in NOAA
b) Requires future acquisitions of Windows based desktops and laptops to include appropriate language regarding the FDCC configuration
c) Provides waiver instructions for organizations that are unable to comply with the FDCC requirements.

Standard secure configurations for OS's other than Windows (e.g., Mac OS, Linux) are envisioned for the near future.

AUTHORITY

This policy is pursuant to and consistent with OMB Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems. Supporting documents include:

(1) Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347).
(2) Cyber Security Research and Development Act of 2002 (Public Law 107-305)
(3) OMB Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
(4) OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations.

INTENDED AUDIENCE

Line Office CIOs, Program and Project Managers, NOAA OCIO staff, network administrators and help desk staff, and persons involved in the procurement of Windows based desktops and laptops.

DESCRIPTION

Secure Configuration Setting for Windows

This policy establishes the FDCC as the standard configuration for NOAA's Windows based desktops and laptops. All Windows based desktops and laptops must be configured in accordance with the FDCC, as maintained by NIST and available at http://csrc.nist.gov/fdcc, no later than February 1, 2008, or obtain a waiver in accordance with the procedures outlined below.

This policy is based on NIST SP 800-68, SP 800-70 and SP 800-53. Additional information such as configuration guidance and recommended scanning tools can be located on the NIST Benchmark repository (http://checklists.nist.gov).

1. Acquisitions of NOAA Windows-based Desktops and Laptops

All NOAA acquisitions of Windows based desktops and laptops (to include routine technical refreshes) shall include contract language, as appropriate, to ensure that the deliverables will comply with the OS configuration mandated by this policy.

OMB Memorandum M-07-18 provides recommended contract language, which may be modified or replaced with similar language as needed at the discretion of Line Office CIOs.

2. Waivers

In the event that compliance with this policy is not possible or practical, offices may apply for a waiver of one or more requirements of this policy. The waiver request must be fully justified and supported by the organization's Chief Information Officer (CIO). Waivers may apply to a defined class of personal computers and/or laptops. The waiver may be in memorandum format, and must provide the following information:

1) A brief rationale for non-compliance with the NOAA standard desktop configuration;
2) A brief statement of the adverse impact or risk of implementing the NOAA standard desktop configurations on critical business processes and IT resources;
3) Identification of any impacts on other NOAA critical business processes, including those of outside agencies and third parties;
4) For class waivers, include a concise description of the scope of personal computers and/or laptops included within the waiver request, and
5) Projected date for compliance.

The NOAA CIO will make the final approval for all waiver requests.

ROLES AND RESPONSIBILITIES

The NOAA CIO Council is responsible for reviewing and approving all proposed changes to this policy. In support of this responsibility, the NOAA Enterprise Architecture Committee is responsible for

maintaining the policy content (to include vetting of proposed changes, providing recommendations to the CIO Council, etc.), in consultation with the NOAA IT Security Committee.

Line Office CIOs are responsible for:

1) Ensuring transition to and implementation of the current FDCC configuration as specified in this policy, and for maintaining compliance with the policy over time, and
2) Coordinating with Contracting Officers as needed to ensure appropriate contract language in all acquisition packages for new Windows based desktops and laptops includes appropriate language that requires deliverables to comply with the OS configuration mandated by this policy, prior to approving the acquisition.

The NOAA OCIO is responsible for reviewing and resolving waiver requests in a timely manner, with support from the NOAA ITSO and/or IT Security Committee as appropriate.

COMPLIANCE

Compliance will be gauged through automated audits as directed by the NOAA CIO.