Managing the Configuration of Information Systems with a Focus on Security

Organizations have to make frequent changes to their information systems in order to implement new and updated hardware and software components, correct software flaws and other errors, address new security threats and adapt to changing business objectives. These constant changes result in adjustments being made to the configuration of information systems; these activities could have an impact on the security of the systems and operations.

In developing information systems, organizations employ many components that can be interconnected in different arrangements to meet the organization's business, mission and information security needs. To protect information systems and information, organizations need techniques for the secure configuration, operation and management of system components, including mainframes, workstations, servers, networks, operating systems, middleware and applications, and for the management and control of risks to systems and information.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has issued a new guide to help organizations develop a well-defined process for managing and controlling secure system configurations and for managing risks in information systems.

Included in this ZIP file are:
- Intro Page.pdf
- Terms and Conditions.pdf
- Secure Configuration Management of Information Systems.pdf