**Common System Harding Recommendations:**

* Use a file system that supports file-level permissions and auditing.
* Disable the guest account in Microsoft Windows and rename the Administrator account. In UNIX, establish policies whereby the root account is never used directly but administrators must issues the **su** command to obtain root access, creating a log of their events in the process.
* Define a complex password for all accounts, do not leave any account with a default password or a blank password.
* Configure account lockout policies and define a logon warning banner.
* Impose organization-specific security limitations, such as blocking Universal Serial Bus (USB) drives or using white list execution management, this is often performed using a security template file.
* Remove all unnecessary protocols.
* Uninstall all unnecessary applications and services.
* Install all available final release updates, patches, fixes, service packs, and other such security measures for the operating system and every remaining application and service.
* Update all hardware device firmware or basic input/output system (BIOS) with the last final release from the vendor.
* Install the latest final releases of all device drivers.
* Install and update antivirus and antimalware scanners.
* Install and configure a host firewall.
* Configure system monitoring and auditing.
* Synchronize the clock.
* Configure communication encryption.
* Run vulnerability assessment tools against the host, such as HFNetChkPro and Nessus.
* Configure regular backups.

**System Hardening Guidelines and Standards:**

* **Defense Information Systems Agency (DISA)**: Department of Defense’s (DoD's) DISA is the largest, and perhaps the best, collection of free Security Technical Implementation Guides (STIGs), hardening instructions, checklists, whitepapers, tools, scripts, policies, and other guidelines.
<http://iase.disa.mil/stigs/index.html>
* **National Institute of Standards and Technology (NIST)**: It is based on National Security Agency (NSA) guidelines, hardening documents, security checklists, and STIG resources. NIST also has a “Gold Standard.” .inf security template available for download. Though not as up to date as the DISA Gold Standard, it goes through a thorough vetting process among various government agencies.
<http://csrc.nist.gov/itsec/guidance_W2Kpro.html>
* **The Center for Internet Security (CIS)**: It is a nonprofit enterprise with a mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls. The practical CIS Benchmarks support available high-level standards that deal with the "why, who, when, and where" aspects of information technology (IT) security by detailing "how" to secure an ever widening array of workstations, servers, network devices, and software applications in terms of technology specific controls. CIS has free tools available to help you determine how your systems currently measure up to their industry standard security baselines.
<http://www.cisecurity.org/>
* **National Security Agency (NSA)**: Central Security Service (CSS)/NSA has developed and distributed configuration guidance for a wide variety of software from open source to proprietary software. The objective of the configuration guidance program is to provide NSA's customers with the best possible security options in the most widely used products.” The NIST STIGs are used as starting points.
<http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/index.shtml>
* **Control Objectives for Information and related Technology (COBIT)**: COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT has become the integrator for IT best practices and the umbrella framework for IT governance because it is harmonized with other standards and is kept up to date.
<http://www.isaca.org/cobit>
* **Policy and Guidance**: It links to various IT security-related policies. It is a good starting point for researching IT security regulations that apply to U.S. military and civilian agencies.
<http://iase.disa.mil/policy-guidance/index.html>
* **SearchCIO.com**: It consists of compliance definitions and acronyms.
[http://searchcio.techtarget.com/sDefinition/0,290660,sid19\_gci947386,00.html](http://searchcio.techtarget.com/sDefinition/0%2C290660%2Csid19_gci947386%2C00.html)
* **Microsoft Security Compliance Manager**: It helps in planning, deploying, operating, and managing security baselines for Windows client and server operating systems and Microsoft applications. It allows to access the database of Microsoft recommended security settings, customize baselines, and then export the baselines to the environment. It also helps in automating the security baseline deployment and compliance verification process.
<http://www.microsoft.com/en-us/download/details.aspx?id=16776>
* **Macintosh Operating System (Mac OS) X Security Configuration Guides**: It provides an overview of features in Mac OS X for hardening your computer. The guides are designed to give instructions and recommendations for securing Mac OS X and for maintaining a secure computer.
<http://www.apple.com/support/security/guides/>