# Global Information Assurance Certification Paper

# How to Develop Your Company's First Security Baseline Standard

Gene Livingston
November 6, 2000



## Introduction

The goal of this document is to provide a guide for those charged with designing and implementing baseline security standards for the first time. The scope of the standards will depend on the immediate needs of the organization, and will specify a standard for installing, hardening, and placing into production, new servers and workstations. On some networks, you can tell who built a particular system by the output of an NMap scan! Some administrators attempt to turn off a few services, others turn them all off, and still others turned the wrong ones off. A Minimum Security Baseline Standard (MSB's) will allow organizations to deploy systems in an efficient and standardized manner.

Creating and maintaining your security baseline standards will be an ongoing process, requiring the help and support of a number of departments within the IT organization. The main goal of developing a security baseline is to promote and strengthen the security of the organizations computing assets. If you are developing MSB's in your organization for the first time, it may be happening in conjunction with the creation of your first security policy, or the creation of your first IT Security Department. The adoption of MSB's can be a useful part of your sites' security policy.

## How your site can benefit from MSB's?

Setting standards for various types of systems will help to enhance host security, allow a more efficient use of time, and make it easier to provide technical support to users by requiring that systems comply to a configuration that has been tested and known to work with the applications used by the organization. Since the help desk will be working with systems complying with the standards (or at least began their working life in a known configuration), they will be more efficient in solving user issues. Please note that there is also a downside to standardization. If all of your systems are configured in the same way, they may ALL become vulnerable to attack in the same manner! This also means however, than you can more easily define the weaknesses within your site.

**How is an MSB different than a Security Policy?**
The MSB's are a how-to on making the security policy work for the site. The MSB's will reflect the goals of the security policy, offering guidelines for preparing individual systems for production use. The MSB's will NEVER conflict with the security policy, and will provide more detail than the security policy. The MSB's are a tool to implement the ideals and goals of the security policy.

**Two Types of Baseline Standards**
There are two important types of security baselines: High-level and Technical. You may decide to develop either or both of these, depending on the needs of your site. The high level standards will be OS independent, broad reaching, and will reflect the goals and mandates of the security policy. It will spell out an achievable baseline as it applies to systems of various security-levels. A good strategy for implementing baseline standards in a company where security-awareness is beginning to bloom is to start with a simple, easy to implement baseline, then tighten up the configurations as needed. Smaller sites may choose to adopt only the technical standards. The technical baselines will consist of separate documents for each type of system used by the organization. This will require the identification of all the different OS configurations used by the company, and the function of each system type. The documents should be classified according to functional type, such as web server, application server, desktop workstation, etc. (See example outlines of both high-level and technical baselines at the end of this document).

A quick starting point for developing your technical standards is to use a system-hardening guide for each OS type, using the parts that fit the needs of your site. These guides can also help you consider issues that you might not have considered. Several links to system hardening guides are listed below:

Linux: http://www.linuxdoc.org/HOWTO/Security-HOWTO.html
Sun Solaris: http://www.softpanorama.org/Security/sos.shtml
MS Windows NT: http://www.upenn.edu/security-privacy/standards/ntConfig.html

Keep the MSB's relevant by keeping up with the needs of your site and be sure that the standards address the 'Top Ten Threats' (http://www.sans.org/topten.htm ) and deals with them.

The next step is to try the MSB configuration against several test machines. This will help identify and correct confusing directions, and insure that your configuration will result in a usable system. After you are satisfied with the technical standard, have the configuration team use the document on a test basis and continue to tune the document.

**How to Ensure Success**

One of the leading causes of death of standards is creating policies that are too rigid. Make sure the technical baseline is reasonable, or you'll be taking the risk that it will become 'another failed IT initiative'.

Make sure that the MSB's are easy to use by making them easily available, along with the scripts, software tools, etc. that are recommended in MSB's. Make the standards available on a company intranet web server and provide links to other related system configuration documents and tools. This will help streamline the configuration process. Build an FTP server that serves up the patches, hot-fixes, logging software and add-on security software to help ensure that the correct software and version is used.

**Conclusion**

Adopting standards for server and desktop systems is one step in developing a more-secure computer network. A secure IT infrastructure is a more efficient infrastructure. Convincing an organization to adopt security baseline standards will result in risk reductions by eliminating the "low-hanging fruit" vulnerabilities, and will make sure that new systems begin service in a known-state. MSB's will help the support team by giving them standard systems to work with. MSB's are a tool to help achieve the goals of the security policy. If designed and implemented properly, MSB's will help strengthen host security, and will help to minimize the damage in the event of a network compromise.

**Appendix A: High-Level Standards Outline**

Some Company High-Level Standards Document

I. Introduction
II. General Guidelines
III. Approved Hardware
IV. Approved Software
I. Application Security Guidelines

**Appendix B: Technical Standards Outline**

Some Company Minimum Technical Standards

I. Introduction
II. Proper base OS install
III. Modifications to file/directory permissions
IV. Services to disable

V. Approved Protocols
VI. Account Policies
VII. Password Policies
VIII. System Auditing

## References

(1)AusCERT. *Information Security Standards*. May 2000.
http://www.auscert.org.au/Information/standards.html

(2) National Computer Security Center (NCSC*). A Guide to Understanding Configuration Management in Trusted Systems*. (Amber Book). March 1988.
http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-006.html

(3) Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual*. July 2000.
http://www.bsi.bund.de/gshb/english/menue.htm

## Suggested Reading

Allen, Julia. Securing Networked Systems – A technology Improvement Process. March, 1999
http://www.cert.org/sepg99/index.htm

Hernan, Shawn. Security Often Sacrificed for Convenience
http://www.stsc.hill.af.mil/crosstalk/2000/oct/hernan.asp

The Experts' Consensus. How to Eliminate The Ten Most Critical Internet Security Threats. September 2000.
http://www.sans.org/topten.htm

Internet Engineering Task Force. Site Security Handbook (RFC 2196). September, 1997.
http://www.ietf.org/rfc/rfc2196.txt