the CENTER for
INTERNET SECURITY

Security Configuration Benchmark For

Cisco IOS Internet Edge

Version 1.0.0
September 2011

http://cisecurity.org
feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for <Target Name> <Target Version>*, provides prescriptive guidance for establishing a secure configuration posture for *<Target Name>* versions *<Target Version>* – *<Target Name>* running on *<Platform>*. This guide was tested against *<Target Name>* *<Target Version>* as installed by WHICH PACKAGE OR TAR. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate *<Target Name>* on a <Platform> platform.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author	**Justin Opatrny**
Maintainers	**Justin Opatrny, Chris Jackson**
Editors	**TBD**
Testers	**TBD**
Contributors and Reviewers	**TBD**

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1. Recommendations

1.1 Develop Zones to Protect Against Attacks

Description:
Cisco IOS (starting in version 12.4(6)T now provides Zone-based Policy Firewall (ZFW) functionality.

A zone defines the boundary of each network based on the level of security necessary for a particular zone.

Rationale:
The ZFW has an advantage over the typical stateless in and out ACLs as it is more configurable and reusable as the applications are based on interzone communications instead of just into or out of an interface.

In addition to providing ACL services, the ZFW includes services including but not limited to stateful packet filtering, URL filtering, and Denial of Service (DoS) mitigation, application inspection and control.

1.1.1 Define Zones (Level 2, Scorable)

Description:
Define each zone that will be in use on the router.

Rationale:
The number of zones will depend on each organization's architecture. The basic zones that are necessary for the Internet Edge are Untrust (Internet facing) and Trust (Internal network).

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to define a zone…

```
hostname(config)# zone security <zone_name>
```

Audit:
Perform the following to determine if the appropriate zone(s) are set properly:

```
hostname# sh run | incl zone security
```

Default Value:
Zones are not defined by default.

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.2 Define Access List (Level 2, Scorable)

Description:
Define an access control list (ACL) to define the allowed paths for a zone.

Rationale:
The allowed paths (device(s), network(s), and/or protocols) for each zone will depend on each organization's architecture.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to define an access list…

```
hostname(config)# access-list <access_list_number_or_name>
<permit|deny> <protocol> <source> <destination> [log]
```

Audit:
Perform the following to determine if the appropriate ACL(s) are set properly:

```
hostname# sh ip access-list
```

Default Value:
Access lists are not defined by default.

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.3 Define Class(es) to Inspect (Level 2, Scorable)

Description:
Each class-map requires inspection of one or more protocols.

Rationale:
The layer 3 and 4 allowed paths chosen will depend on the organization's security policy.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to define a class-map...

```
hostname(config)# class-map type inspect {match-any | match-all }
<class_map_name>
```

Audit:
Perform the following to determine if the necessary class-map is defined:

```
hostname# sh run | incl class-map type
```

Default Value:
A class-map is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.3.1 Define Protocol(s) to Inspect (Level 2, Scorable)

Description:
Each class-map requires inspection of one or more protocols.

Rationale:
The protocols chosen will depend on the organization's security policy.

Platform: IOS

Dependencies:

IOS: 1.1.3 Define Class(es) to Inspect

Remediation:
Perform the following to define a class-map...

```
hostname(config-cmap)# match protocol <protocol_name>
```

Audit:
Perform the following to determine if the necessary protocol is defined:

```
hostname# sh run | incl match protocol
```

Default Value:
A match protocol is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.3.2 Define Access-Group to Inspect (Level 2, Scorable)

Description:

Each class-map requires inspection of one or more access-groups.

Rationale:
The access-groups developed and chosen will depend on the organization's security policy.

Platform: IOS

Dependencies:

IOS: 1.1.2 Define Access List

1.1.3 Define Class(es) to Inspect

Remediation:
Perform the following to define an access-group...

```
hostname(config-cmap)# match access-group <access_list_number_or_name>
```

Audit:
Perform the following to determine if the necessary access-group is defined:

```
hostname# sh run | incl match access-group
```

Default Value:
An access-group is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.4 Define Policy to Inspect (Level 2, Scorable)

Description:
Define a policy map.

Rationale:
This is a required step in developing a ZFW policy.

Platform: IOS

Dependencies:
IOS: None

Remediation:
Perform the following to define a policy-map...

```
hostname(config)# policy-map type inspect <policy_map_name>
```

Audit:
Perform the following to determine if the necessary inspect policy-map is defined:

```
hostname# sh run | incl policy-map type
```

Default Value:
A policy-map is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.4.1 Define the Class to Inspect (Level 2, Scorable)

Description:
Each policy-map evaluates traffic based on one or more class-maps

Rationale:
The class-map(s) chosen will depend on the organization's security policy.

Platform: IOS

Dependencies:

IOS: 1.1.4 Define Policy to Inspect

Remediation:
Perform the following to define a policy-map...

```
hostname(config-pmap)# class type inspect <class_map_name>
```

Audit:
Perform the following to determine if the necessary class-map is defined:

```
hostname# sh run | incl class type
```

Default Value:
A class type is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.4.1.1 Set the policy-map Class to Inspect (Level 2, Scorable)

Description:
Define each class type to inspect

Rationale:
This enables the policy-map to inspect the traffic

Platform: IOS

Dependencies:

IOS: 1.1.4 Define Policy to Inspect

1.1.4.1 Define the Class to Inspect

Remediation:
Perform the following to set inspection for a policy-map...

```
hostname(config-pmap-c)# inspect
```

Audit:
Perform the following to determine if the necessary inspection is defined:

```
hostname# sh policy-map
```

Default Value:
A class type is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.5 Define the Zone Mapping (Level 2, Scorable)

Description:
Interzone traffic requires a defined mapping.

Rationale:
Mapping of the zones allows for the granular definition of which zone uses which policy.

Platform: IOS

Dependencies:

IOS: 1.1.1 Define Zones

1.1.4.1.1 Set the policy-map Class to Inspect

Remediation:
Perform the following to map interzone traffic...

```
hostname(config)# zone-pair security <zone_pair_name> source
<source_zone> destination <destination_zone> service-policy type
inspect <policy_map_name>
```

Audit:
Perform the following to determine if the necessary zone-pair is defined:

```
hostname# sh run | incl zone-pair
```

Default Value:
A zone-pair is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.5.1 Define a Description of the Zone Mapping (Level 2, Scorable)

Description:
Provide a description for each zone-pair.

Rationale:
A description provides a more detailed understanding of the purpose of the zone-pair as this level of detail is not typically appropriate (due to size) for name of the zone-pair itself

Remediation:
Perform the following to set the zone-pair description...

```
hostname(config-sec zone-pair)# description <zone_pair_description>
```

Audit:
Perform the following to determine if the necessary class-map is defined:

```
Hostname(config)# sh run | incl description
```

Default Value:
A zone-pair description is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.5.2 Define the Policy to Inspect in the Zone Mapping (Level 2, Scorable)

Description:
Interzone traffic requires a define mapping.

Rationale:
Mapping of the zones allows for the granular definition of which zone uses which policy.

Platform: IOS

Dependencies:

IOS: 1.1.4.1.1 Set the policy-map Class to Inspect

1.1.5 Define the Zone Mapping

Remediation:
Perform the following to map interzone traffic...

```
hostname(config-sec zone-pair)# service-policy type inspect
<policy_map_name>
```

Audit:
Perform the following to determine if the necessary policy-map is defined:

```
hostname# sh run | incl service-policy
```

Default Value:
A zone-pair service-policy is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.1.6 Apply Zone to Appropriate Interface (Level 2, Scorable)

Description:
Each interface requiring ZFW services must apply a zone to the interface itself.

Rationale:
The zone applied to the interface will depend on the security level of the applications and/or device(s) attached to that network.

Platform: IOS

Dependencies:

IOS: 1.1.1 Define Zones

Remediation:
Perform the following to apply a zone to an interface...

```
hostname(config)# int <interface>
hostname(config-if)# zone-member security <zone_name>
```

Audit:
Perform the following to determine if the necessary zone is applied to the interface:

```
hostname# sh run int <interface> | incl zone-member
```

Default Value:
A zone-member is not configured by default

References:

1. Zone-Based Policy Firewall Design and Application Guide
2. Cisco IOS Security Command Reference

1.2 Increase Administrative Restrictions

Description:
Due to the router being at the Internet Edge, there is sufficient need to increase specific requirements around administration of the router.

1.2.1 Require a Minimum Password Length (Level 2, Scorable)

Description:
Require a password of at least 15 characters.

Rationale:
In conjunction with encrypted administrative access, increasing the length of a complex password will decrease the potential for cracking. This should be in conjunction with encrypted remote administration protocols (e.g. SSH).

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to require a minimum password length...

```
hostname(config)# security passwords min-length <length>
```

Audit:
Perform the following to determine if the password length is applied:

```
hostname# sh run | incl min-length
```

Default Value:
A minimum password length is not configured by default

References:

1. Network Security Baseline
2. Cisco IOS Security Command Reference

1.2.2 Require a Delay between Login Attempts (Level 2, Scorable)

Description:
Require a delay between login attempts.

Rationale:
Increasing the time between login attempts decreases the speed of password attacks.

This should be in conjunction with encrypted remote administration protocols (e.g. SSH).

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to require a delay...

```
hostname(config)# login delay <length_in_seconds>
```

Audit:
Perform the following to determine if the login delay is applied:

```
hostname# sh run | incl delay
```

Default Value:
A login delay is not configured by default

References:

1. Network Security Baseline
2. Cisco IOS Security Command Reference

1.2.3 Create an Internet Edge ACL to Protect the Untrust Interface (Level 1, Scorable)

Description:
Create ACL to protect the router's untrusted interface, next hop routing communications, and against anti-spoofing.

Rationale:
The Internet Edge router is the first line network defense and limits general types of traffic from entering the network and restricts source/destination of border routing protocols.

Platform: IOS

Dependencies:

IOS: None

Remediation:
Perform the following to create the ACL...

```
hostname(config)# ip access-list extended <internet_edge_acl_name>
hostname(config-nacl)# deny tcp any <internet_edge_network>
<internet_edge_network_wildcard_mask > fragments
hostname(config-nacl)# deny udp any <internet_edge_network>
<internet_edge_network_wildcard_mask > fragments
```

```
hostname(config-nacl)# deny icmp any <internet_edge_network>
<internet_edge_network_wildcard_mask > fragments
hostname(config-nacl)# <anti-spoofing_acl_lines_from_baseline_document>
hostname(config-nacl)# permit tcp host <internet_edge_router_ip> host
<bgp_peer_router_ip> eq bgp
hostname(config-nacl)# permit tcp host <internet_edge_router_ip> eq bgp
host <bgp_peer_router_ip>
hostname(config-nacl)# deny ip any <internet_edge_network>
<internet_edge_network_wildcard_mask>
hostname(config-nacl)# permit ip any any
```

Audit:
Perform the following to determine if the necessary zone is applied to the interface:

```
hostname# sh ip access-list extended <internet_edge_acl_name>
```

Default Value:
An Internet Edge ACL is not configured by default

References:

1. Network Security Baseline
2. Cisco IOS Security Command Reference

1.2.3.1 Apply the Internet Edge ACL (Level 2, Scorable)

Description:
Apply the ACL to protect the router's external interface and next hop communication.

Platform: IOS

Dependencies:

IOS: 1.2.3 Create an Internet Edge ACL to Protect the Untrust Interface

Remediation:
Perform the following to protect the external interface...

```
hostname(config)# interface <external_interface>
hostname(config-if)# ip access-group <internet_edge_acl_name> in
```

Audit:
Perform the following to determine if the necessary ACL is applied to the interface:

```
hostname# sh ip int <external_interface> | incl Inbound
```

Default Value:
An Internet Edge ACL is not applied to an interface by default

References:

1. Network Security Baseline
2. Cisco IOS Security Command Reference

1.2.4 Restrict Administrative Access to Trusted Interface (Level 2, Scorable)

Description:
Bind administrative access of the Internet Edge router to the trusted interface

Rationale:
Minimize the risk of external attacks against administrative features by restricting access to administrative functions such as SSH or SNMP, to the trusted interface.

Platform: IOS

Dependencies:

IOS: 2.3.3.1.1 Enable Cisco Express Forwarding (CEF) – IOS Baseline

Remediation:
Perform the following to define an in-band management interface...

```
hostname(config)# control-plane host
hostname(config-cp-host)# management-interface <trusted_interface_type>
<trusted_interface_number> allow <mgmt_protocol_1> [mgmt_protocol_2]
[...]
```

Audit:
Perform the following to determine if the in-band management interface is defined:

```
hostname# sh run | incl management-interface
```

Default Value:
A management interface is not configured by default

References:
1. Cisco Guide to Harden Cisco IOS Devices
2. Understanding Control Plane Protection

Appendix A: References

1. Cisco Systems, Inc. (2010). Cisco IOS Firewall – Zone-Based Policy Firewall Design and Application Guide. http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml. Last accessed July 24, 2011.

2. Cisco Systems, Inc. (2010). Cisco Guide to Harden Cisco IOS Devices. http://www.cisco.com/image/gif/paws/13608/21.pdf. Last accessed August 8, 2011

3. Cisco Systems, Inc. (2010). Understanding Control Plane Protection. http://www.cisco.com/web/about/security/intelligence/understanding-cppr.html. Last accessed August 8, 2011.

4. Cisco Systems, Inc. (2010). Enterprise Internet Edge. http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/chap6.html. Last accessed August 8, 2011.

5. Cisco Systems, Inc. (2011). Cisco IOS Security Command Reference. http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html. Last accessed September 7, 2011

Appendix B: Change History

Date	Version	Changes for this version
July 24, 2011	0.1	ZFW section development
July 27, 2011	0.2	Password section development
August 8, 2011	0.3	Internet Edge ACL and MPP development
August 23, 2011	0.4	Added additional working to description and rationale sections
August 23, 2011	0.4	Corrected wording in several audit sections
September 7, 2011	0.5	Corrected inconsistencies in several sections
September 7, 2011	0.5	Added missing reference