

CDI Information Security Policy

To: ITD

No.: ISO-05

From: Information Security Office (ISO)

Issued: August 1, 2004

Subject: Hardening and Updating Policy

Expires: When Superseded

Policy

It is the policy of the California Department of Insurance (CDI) that all operating system upgrades (including but not limited to CDI servers, routers and firewalls) must be appropriately planned, evaluated for compatibility and security, tested and approved by the Information Technology Division (ITD) prior to any acquisitions and/or procurements of upgrades. Requests for software upgrades should be handled as directed by ITD ([See IT Circular 04-05](#)).

It is also the policy of CDI that all software and systems shall have current security patches/updates applied in a timely manner. To keep current on software and system patches/updates, the ISO staff will continue to subscribe to various free security mailing lists (e.g. BugTraq, SANS, CIAC, Infragard, etc.) and monitor reputable security sites (e.g. U.S. or California Department of Homeland Security, California State ISO, CIAC, CERT, SANS, NIST, Microsoft, etc.) on a regular basis. The ISO staff will provide ITD with timely information regarding security patches/updates for software and systems used by CDI.

Purpose

To ensure that all CDI servers, routers, desktops and firewalls are adequately protected against all current vulnerabilities using best practices and industry standards, and to protect all sensitive and critical information assets within CDI.

Software and Systems Under CDI's Control

To mitigate risks to CDI software and systems, all patches/updates for software and systems under CDI's control, that are listed as "high" or "critical", shall be tested and applied as soon as ITD has been informed by the ISO and made the decision that it is safe to deploy.

Firewall, Server and Router Security

It is the policy of CDI that all firewalls, internal servers, routers and other security devices or systems must be known to, mapped, and documented by ITD. Approved configuration guidelines shall be established, documented, and

maintained by the Statewide Network Support Bureau for each firewall, server and router.

All firewalls, servers and routers must have documentation. At a minimum, the following information is required:

- Name of contact(s) and location, along with a back-up contact;
- Hardware operating system/version;
- Main function and application, if applicable;
- Configuration changes to firewalls, servers and routers must be logged, and the appropriate change control procedures must be followed;
- The ISO's review and signoff of all configuration changes to ensure that they are consistent with good security practices.

General Configuration Guidelines

The general configuration of all CDI firewalls, servers and routers shall:

- Be in accordance with approved information security best practices (i.e. IEEE, ISO 17799, NIST, SANS, etc.) as specified by the ISO;
- Operate under the principle of least access or privilege;
- Be installed with all services, ports or applications closed. (Only service ports or applications necessary for CDI business needs shall be opened);
- Have access to services logged and/or protected through access-control methods;
- Have the most recent security patches/updates downloaded, tested and installed on it as soon as practical. (The only exception being when immediate application would interfere with business requirements or operations, or if the patch/update failed to test compatible to the CDI environment);
- Limit the use of trust relationships between systems when another method of system communication can be used;
- Not use root or administrator privileges when a non-privileged account can be used;
- Be physically located in an access controlled area (CDI firewalls, servers, and routers are specifically prohibited from operating from uncontrolled cubicles or office areas);
- Not be connected to the CDI network without the approval of ITD;

Hardening and Configuration of Firewalls, Servers, Routers and Other Security Devices or Systems

It is the policy of CDI that all firewalls, servers, routers and other security devices or systems shall be hardened ([SAM Section 5310 #5\(e\)- Information Integrity, and Security](#)). In addition, all default passwords shall be changed, unnecessary ports shall be closed, and unnecessary services turned off prior to being connected to the CDI network. Any change to the configuration of a firewall,

server, router, other security device or system or the application of a security patch/update requires the System Administrator to verify and document that the device or system has not reverted to a default, open or unhardened state as a result of the change. Firewalls, servers, routers and other security devices or systems may not be connected to the CDI network without the approval of ITD.

Documentation of the hardening and the configuration of the firewall, server, router and other security device or system must be kept by ITD. Documentation of changes made to firewalls, servers, routers or other security devices or systems under CDI's control must include the following:

- The name and location of the firewall, server, router, or other security device or system;
- The hardware and operating system/version;
- The main function and applications running, if applicable;
- The name or user ID of the person making the change;
- The date and time of the change;
- The changes made;
- Verification that the change has not left the device or system in a default, open or unhardened state;
- The signature of the person making the change and verifying the hardening;

Procedure

ITD will develop and maintain procedures.

Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3261 if you have any questions regarding this policy.

Archie Alimagno, Information Security Officer