HISPOL 003.0

The United States House of Representatives Information Security Policy for Connecting to the House Local Area Network

Version:	**2.0**
Approved:	**August 2006**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

Rapid advancements in technology have made the United States House of Representatives (House) increasingly dependent on interconnected information systems to store, process, and distribute vast quantities of valuable, sensitive, and critical data. With the expansion of the Internet and the increasing use of Internet technology within the House, systems can potentially be reached from both the outside and inside the House environment. The Internet is an exponentially growing "network of networks" linking military, government, academia, and commercial information systems in countries worldwide. It also serves as a hub for global electronic mail (email) interconnection, providing a network of immense power. The House Intranet is a private network consisting of interlinked local area networks. The Intranet allows the House community to share information among Members, Committees, Officers, and staff. As connectivity increases, so does the risk of attack on the network. Two principles should guide and govern a network security system - the need to maintain the integrity of data communications and the need to protect information assets.

Because the House Intranet is a private network, appropriate security measures continue to be implemented; ensuring adequate safeguards are in place to mitigate potential risks. However, as a public network the Internet is vulnerable to monitoring of information or use by unauthorized parties. Networks connected to the Internet are particularly vulnerable to attacks that can result in denial of services, unauthorized access to confidential information, and the introduction of computer viruses or other malicious code that disrupt network operations.

The goal of this policy is to minimize internal and external security threats to House information systems while allowing House Offices to use the campus Intranet, Internet, and other external networks to the maximum extent feasible.

1.1 Scope

This document provides all users of House information systems with guidance governing permanent connections to the local area network (LAN), Internet and Intranet security. All House Offices, employees, and contractors that connect to the House LAN and utilize House information systems must follow this policy guidance since improper use of information systems can potentially put the entire House network at risk.

2 Policy Guidelines

All House Offices must notify the Information Systems Security Office (ISSO) when connecting systems to the House network. Audits will be conducted on new systems and systems that undergo major modifications prior to implementation and on existing systems every two (2) years. If an audit reveals significant vulnerabilities, corrective action must be taken within the period specified by the ISSO.

- Any device or component with a permanent connection to the House network shall be used for authorized purposes, only, and may not be used for campaign, political, or commercial activities. Use of such devices and components must comply with House Rules and the guidance of the Committee on Standards of Official Conduct.
- Any device or component with a permanent connection to the House network, or to the overall House infrastructure must be reviewed and approved to minimize the potential for security risks and violations.
- Permanent connections to the Internet outside of the House infrastructure must be reviewed and approved by the Information Systems Security Office. All Internet access and servers attached to the House LAN must comply with House policies, procedures, technical specifications, and guidelines and must pass through the House maintained security infrastructure.
- Only Members, Officers, and employees are authorized to connect to the House LAN using a permanent connection, as defined in this policy.
- Modems are not permitted for use at the House unless authorized by the ISSO, except when connected to a fax machine, since the devices may be used to bypass security features, such as firewalls, designed to keep unauthorized users from accessing the network.
- All House Office information systems connecting to the House network infrastructure must be physically and logically isolated from vendors external to the House and all other non-House networks, unless explicitly validated by the ISSO.
- All House offices must ensure that servers are located within areas of minimal public and visitor traffic.
- All House Offices authorized with a permanent connection to the LAN and access to the Internet must designate a central point of contact (POC) for all matters pertaining to their connection. In most cases, the system administrator is the designated POC.
- All new public web sites for Members or Committees must be hosted on a server managed by HIR, or by an authorized vendor if the server is located on the House Campus.
- All public Web sites must be registered with the ISSO and the Communications Office. Internet access will not be approved until the registration process has been completed.
- A mail server may only use approved House mail relay servers if the message originates from a computer physically connected to the House network**.** No mail server shall be allowed to utilize third party mail systems for any Simple Mail

Transfer Protocol (SMTP) traffic outside of the House domain. This policy is enforced at the House firewalls.

- All programs used on the system must be checked prior to installation for viruses or other malicious forms of code. This is especially important for programs received from outside sources, including the Internet. Each House Office must have the House-provided or an equivalent current anti-virus program installed on their systems.
- It is the responsibility of each House Office to contact the ISSO and report security incidents, such as unauthorized access or unusual system activities, to the House Computer Incident Response Team (House CIRT). The House CIRT will conduct an investigation, provide recommendations to resolve the incident, and follow up with the designated POC to ensure corrective actions are completed.