HISPOL 003.0

The United States House of Representatives Internet/ Intranet Security Policy

CATEGORY: Telecommunications Security

ISSUE DATE: February 4, 1998
REVISION DATE: August 23, 2000

The United States House of Representatives
Committee on House Administration

Title: United States House of Representatives – Internet/Intranet Security Policy

Number: HISPOL – 003.0

Category: Telecommunications Security

Date: February 4, 1998
Revision: August 23, 2000

Status: Approved – Committee on House Oversight
Revision Approved – Committee on House Administration

Purpose:

The purpose of the United States House of Representatives – Internet/Intranet Security Policy is to provide the House community with procedures to access and guidelines to secure Internet and Intranet services.

THIS POLICY DOES NOT SUPERSEDE REQUIREMENTS OF HOUSE RULES WHICH GOVERN THE ACTS OF ALL EMPLOYING AUTHORITIES OF THE HOUSE.

Audience:

This document has relevance to all U.S. House of Representatives Members, employees, offices, and contractors who routinely use or have occasion to use House Internet/Intranet connections.

References:

HISPOL 002.0 – U.S. House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use

HISPOL 002.1 – U.S. House of Representatives General Information Security Guidelines to Protect Member and Committee Office Systems from Unauthorized Use

HISPOL 005.0 – U.S. House of Representatives General Information Security Policy for Vendor Remote Access to the House Network

HISPOL 005.1 – U.S. House of Representatives General Information Security Policy for Connectivity to the House Network

Table of Contents

1.0 INTRODUCTION

Rapid advancements in technology have made the U.S. House of Representatives (House) increasingly dependent on interconnected information systems to store, process, and distribute vast quantities of valuable, sensitive, and critical data. Such information systems are provided to the House via access to the Internet and to the House Intranet. The Internet is an exponentially growing "network of networks" linking military, government, academic, and commercial computers in countries around the world. It also serves as a hub for global electronic mail 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 and computer resources among Committees, Members, Officers, and staff.

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 forms of code which disrupt network operations.

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

2.0 POLICY GUIDELINES

All House Offices must submit to House Information Resources (HIR) a written request to access House Internet or Intranet services. Approval will be given only when the Office has demonstrated compliance with the following guidelines via a completed system-specific security compliance checklist and, as required, an audit by the HIR Information Systems Security Office. Audits are conducted on new systems prior to implementation and on existing systems every two years. Systems that undergo major modifications will also be reviewed prior to implementation.

- All offices must ensure that servers are located in areas with minimum public and visitor traffic.

- All users must use unique logon IDs and utilize effective password security as described in published House security policy.

- All House Offices authorized access to the Internet must designate a person (usually the systems administrator) to be the central point of contact (POC) for all matters pertaining to their Internet/Intranet connection.

- The designated POC must complete and submit to the HIR Information Systems Security Office the appropriate security compliance checklist when a system is initially connected to the House network and every two years thereafter. A new checklist must be completed and submitted by the POC when a new server or operating system is installed on the House network, or when a change in vendor occurs.

- The HIR Information Systems Security Office will issue a revised security compliance checklist when vulnerabilities are identified that might adversely affect the House network. The POC must then complete and submit a revised checklist or change pages, and should implement the recommended configuration changes to ensure maximum protection of House systems.

- House Offices running public web sites not located on an HIR-managed web server or using external servers must register with the HIR Information Systems Security Office and the HIR Communications Office. Internet access will not be approved until registration has been completed. Sites and servers will automatically be registered when the initial system-specific security compliance checklist is submitted to the Security Office.

- 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 Office must have the House-provided or an equivalent current anti-virus program installed on their systems.

- It is the responsibility of each Office to 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 point of contact to ensure corrective actions are completed.

3.0 PROCEDURES FOR ACCESS

To request access to House Internet or Intranet services, the requesting Office should complete the following actions:

- Ensure the recommended policy and technical guidelines found in Sections 2.0 and 4.0, respectively, of this policy have been implemented,

- Submit a letter requesting Internet/Intranet access (House Information Security Form (HISFORM) 002.0),

- Conduct a security audit in accordance with the system-specific security compliance checklist and submit the completed checklist to the HIR Information Systems Security Office for review,

- Submit a completed Security Compliance Verification Form (HISFORM 006.0).

Upon approval, HIR shall ensure:

- Necessary or recommended HIR-provided software is installed,

- Office security protections are reviewed and a written report of findings is completed and provided to the House Office,

- Initial security training is provided on such topics as Internet e-mail vulnerabilities, acceptable password guidelines, and modem vulnerabilities,

- House-provided or an equivalent current anti-virus program is installed,

- Data traffic from the Internet/Intranet to the office subnet is enabled,

- Available HIR Internet/Intranet training is scheduled.

To ensure the continued protection of all servers connected to the House network, failure to comply with the aforementioned procedures may result in the temporary suspension of Internet access or a delay in the approval of initial Internet/Intranet access.

4.0 RECOMMENDED TECHNICAL GUIDELINES FOR SECURING SYSTEMS

The following recommendations must be completed before requesting access to Internet/Intranet services.

- Begin with a clean operating system by installing system software from its original distribution source or completely audit the system software. Remove any accounts that are not actively used and have all users routinely change their passwords. All administrative accounts or login IDs must have the default passwords changed to meet the secure password requirements.

- Every individual should have a unique login account. Sharing accounts interferes with the necessary individual accountability. In order to authenticate that only the responsible individual is using each account, these accounts require password protection. Unauthenticated “guest” accounts are prohibited (except for carefully implemented read-only access) because their actions cannot be attributed to any particular individual.

- Modems should be turned off except when in use and programmed for originating calls only. If a computer with a modem can answer a call, it reduces the security of that computer to only the protection of the users’ passwords.

- When users connect to computers on the House Intranet over communication channels outside the control of the House, stronger authentication than passwords (which could be captured by an attacker) is recommended. Stronger authentication includes methods such as encryption, pre-assigned addresses (e.g. dial-back modems on separate telephone lines), or one-time password generators (i.e., SecurID cards).

- Configure static (default) routes rather than running (routed or gated) processes that learn about IP routes from the network. If a subversive computer on the local network (falsely) advertises a route at lower cost to a destination, it could spoof the communications path and capture confidential information (e.g. passwords). This configuration issue applies mostly to multi-user computers (e.g. Unix), since most single-user computer software uses the default router approach.

- Application programs downloaded from an external untrusted source should not be executed. Anti-virus software should be run on any downloaded code prior to using the application to ensure it is virus-free.

- Offices should periodically backup the entire file system to facilitate recovery if a compromise occurs. Regular backups also make it easier to determine the chronology and nature of an attack. Backup tapes must be kept in a secured fireproof area away from office systems or off-site. Because an attack may not be immediately apparent, Offices should retain two system backups for at least six months.

- System administrators should regularly monitor system security (e.g., routine checks of audit log data) and educate users about the need for continued security awareness. There are various third-party software utility programs that can be configured to audibly notify system administrators when anomalous events are recorded in the audit logs. HIR can provide guidance and information on these applications.

- Continuing security information is available for system administrators via various avenues including the HIR security web page and security newsgroups. In addition, product web sites generally include security patches available for download.

5.0 ACCESS TO OTHER HOUSE INTRANET SERVICES

While the House depends mainly on networked systems, many offices continue to rely on and use systems residing on mainframe computing resources. Policies and procedures regarding access to mainframe resources are found in the *House Information Resources Computer Center Handbook.* Guidance associated with specific Intranet services such as web servers or messaging servers will be developed as needed to augment current House policies and publications.