HISPOL 005.1

The United States House of Representatives Information Security Policy for Connectivity to the House Network

CATEGORY: **Telecommunications Security**

ISSUE DATE: **November 1, 1999**
REVISION DATE: **December 11, 2001**

The United States House of Representatives
Committee on House Administration

Title: United States House of Representatives – Information Security Policy for Connectivity to the House Network

Number: HISPOL - 005.1

Category: Telecommunications Security

Date: November 1, 1999
Revised: December 11, 2001

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

Purpose:

The purpose of the United States House of Representatives – *Information Security Policy for Connectivity to the House Network* is to provide the House user community with a policy governing connectivity to the House network.

Audience:

This document has relevance to all Member, Committees, Leadership, and other House Offices who require a connection to the House network infrastructure.

References:

HISPOL 002.0 – United States House of Representatives General Information Security Guidelines for Protecting Systems from Unauthorized Use

HISPOL 003.0 – United States House of Representatives Internet/Intranet Security Policy

HISPOL 005.0 – United States House of Representatives Security Policy for Vendor Remote Access to the House Network

1.0 INTRODUCTION

Organizations large and small have increased the use of networked computers. Where once only electronic mail was exchanged within or among organizations, now intellectual property, product information, invoices, purchase orders, human resources data, credit card numbers, and more travel over these networks. Networked computers have become critical to the business operations of the House.

With the expansion of the Internet and the increasing use of Internet technology within the House, more and more computing resources have become connected to networks that can potentially be reached both from outside and inside the House environment. As connectivity increases, so does the risk of attack on network resources. 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.

Guidelines for connectivity to the House networks are described in this policy.

2.0 Guidelines for Connectivity to House Networks

The following guidelines for connectivity to the House networks must be observed to ensure the integrity of House-wide systems. All requests and accompanying justifications for network connectivity must be thoroughly reviewed and approved by the House Information Resources (HIR) Information Systems Security Office and the HIR Communications Office prior to implementation.

- 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 HIR infrastructure are prohibited. This includes the use of leased lines and wireless connections. All Internet access must be in compliance with House policies, procedures, and technical specifications (available at http://onlinecao.house.gov/hir-security/hisdocs.htm), and must pass through the House maintained security infrastructure.

- Only Members, Officers, and Employees are authorized to connect to the House network using a permanent connection, as defined above.

- The House Office 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.

- All servers attached to the House network are subject to House policies, procedures, and technical specifications.

- Modems are not permitted for use at the U.S. House because the devices may be used to bypass security features, such as firewalls, designed to keep unauthorized users from accessing the network.

- HIR provides two central services for remote access, dial-in and Virtual Private Network (VPN), both of which require the use of a SecurID card. Offices with a compelling business need to utilize modems are to contact the Information Systems Security Office for assistance in migrating to these central services. Guidance for the secure use of modems is provided in the corresponding House Information Security Publication.

- Each Member, Officer, or employee must ensure his or her systems connected to the House network are protected from unauthorized access, disclosure, transmission, modification, destruction, and bypassing of security measures. New systems must not adversely impact the confidentiality, integrity, availability, or accountability of security services for House systems.

- Computer systems may utilize direct connections to the House network only if utilizing House-authorized security authentication standards and procedures. The currently approved remote access method is via SecurID card. Procedures for obtaining and using a SecurID card are found in the corresponding House Information Security Publication.