HISPOL 005.0

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

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

Table of Contents

1 Introduction 3
1.1 SCOPE 3
2 Remote Access Guidelines 3
3 Vendor Requirements 4
3.1 EXTENSION OF THE HOUSE NETWORK TO VENDORS 4

1 Introduction

Organizations large and small have increased the use of networked computers. Information exchange within or among organizations has expanded well beyond electronic mail (email) to include intellectual property, product information, procurement records, human resources data, etc. traveling over these networks. Networked information systems have become critical to the business operations at the United States House of Representatives (House).

With the expansion of the Internet and the increasing use of information technology within the House, an increasingly number of information systems have been 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 - maintaining the integrity of data communications and protecting information assets. This policy addresses those principles and provides guidelines for connectivity to House information systems and networks.

1.1 Scope

The purpose of this policy is to provide the House community with a policy governing secure remote access to the House network. All House Offices, employees, contractors, and vendors that connect to the House network must follow this policy guidance since improper use of information resources can potentially put the entire House network at risk. This policy also provides rules, regulations, and audit mechanisms for vendors that require remote access to the House network for support and maintenance actions.

This policy does not supersede requirements of House Rules that govern the acts of all employing authorities of the House.

2 Remote Access Guidelines

Currently there are two solutions supported to accommodate secure remote access to the House network. One solution – Secure Modem Bank – is suitable for limited, lower-end support, while the other – Virtual Private Network (VPN) – provides for a high level of support. While both these choices are technically secure, the human element will always be present as an underlying threat to system security.

These two solutions require the use of SecurID two-factor authentication. SecurID two-factor authentication is based on "something the user knows" (e.g., User ID and PIN) and "something the user has" (e.g., SecurID). Successful authentication permits an authorized user access to the network.

The following requirements for connectivity to the House networks must be observed to ensure the integrity of House-wide information systems. All requests and accompanying justifications for network connectivity shall be reviewed and approved

by the Information Systems Security Office (ISSO) and the HIR (House Information Resources) Communications Office prior to implementation.

- Modems, except when connected to a fax machine, are not permitted for use at the House unless explicitly authorized by the ISSO. The devices may be used to bypass security features, such as firewalls, designed to keep unauthorized users from accessing the network.
- Two central services for remote access are provided to the House community - dial-in and Virtual Private Network (VPN) - both of which require the use of secure, two-factor authentication (SecurID). Offices with a compelling business need to utilize modems must contact the ISSO for assistance in migrating to these central services. Guidance for the secure use of modems is provided in the corresponding United States House of Representatives Information Security Publications (HISPUBs).
- Each Member, Officer, employee, contractor, or vendor must ensure his or her system(s) 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 two-factor authentication via SecurID. Procedures for obtaining and using SecurID are found in corresponding HISPUBs.

3 Vendor Requirements

Member, Committee, Leadership, and other House Office information systems face an environment of escalating integration complexity and the need for fiscal constraint. To remain competitive, system integration vendors (hereafter referred to as vendors) that support these systems face the challenge of providing better service and support with the same or fewer personnel. Secure technical solutions designed to facilitate vendor support must be established to meet the needs of both the House and the vendors themselves. The technical issues at hand involve the methods by which vendors may remotely access the House network for support and maintenance actions.

3.1 Extension of the House Network to Vendors

Some vendors require a higher bandwidth connection in order to provide a better grade of service to their House accounts and more efficient utilization of their human resources. In these cases, it is possible to extend the House network to include a direct, point-to-point connection to the vendor. The conditions outlined below must be met for a connection of this nature to be employed.

3.1.1 Vendor Internal Network Controls

- The network being connected to the House for performing contractual work is physically separated from all other internal vendor networks. If the network is the only network at the vendor site, then its sole function must be in support of House contracts.
- All fileservers (including UNIX hosts) attached to the vendor's internal network are subject to the same secure configuration set up, audit controls, and policies as are enforced on House systems.
- No Internet connections (or outside network connections) are permitted on any vendor network that is connected to the House network, except as specifically authorized by the House. If the vendor network requires access to the Internet, it must be authorized by the House via the House network and therefore, will be within the security model and control of the House's firewall protection.
- No direct dial-in (modem) access to the vendor internal network is permitted. Dial-in access by vendor personnel to the vendor's internal network will be accomplished by using the House's secure modem bank and SecurID.

3.1.2 Transmission Medium

- Direct connections to the House network must be via dedicated, point-to-point, non-switched telecommunication lines.
- The vendor assumes all costs incurred with the installation, termination, maintenance, and leasing of the telecommunication line.

3.1.3 Personnel Issues

- All vendor personnel involved in system support and maintenance of House information systems, including Committee, Member, Leadership, and Support Offices are subject to the rules, regulations, and sanctions as outlined in House information security policies.

3.1.4 House Network

- The HIR Communications Office shall provide and control the routed interface.
- Vendor access to House information systems is limited to systems within the vendor's customer base, only. Attempts to access information systems outside the vendor's cognizance will be considered a breach of security and handled accordingly.
- Vendors shall not engage in any network monitoring or management activities without prior approval of the ISSO.

3.1.5 Management, Audit, and Control

- The vendor shall provide either a diagram or a descriptive listing of all computing resources (e.g., workstations, servers, routers, etc.) attached to the vendor network. The House will use this information as the basis for determining connectivity authorization.
- The vendor's internal network will be subject to periodic audits and reviews conducted by ISSO personnel or their designees. These audits may be announced or unannounced visits to the vendor facility for inspection of the physical network plant, procedures, and controls; network-oriented audits; and office audits.