HISPOL 005.0

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

CATEGORY: Telecommunications Security

ISSUE DATE: February 4, 1998

The United States House of Representatives
Committee on House Oversight

Title: United States House of Representatives - Information Security Policy for Vendor Remote Access to the House Network

Number: HISPOL - 005.0

Category: Telecommunications Security

Date: February 4, 1998

Status: Approved – Committee on House Oversight

Purpose:

The purpose of the United States House of Representatives - Information Security Policy for Vendor Remote Access to the House Network is to provide House system integrators with a policy governing secure remote access to the House network. The policy provides rules, regulations and audit mechanisms for two methods of vendor access to the House network: (1) via SecurID/ modem bank, and (2) via direct connection.

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 House system integrators that require remote access to systems located in Member, Committee and other House offices for conducting system support and maintenance actions.

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 004.0 - United States House of Representatives Security Policy for Information System-Related Security Incidents

HISFORM 015.0 - Memorandum of Understanding

Attachment 1 - HISFORM 015.0 - Memorandum of Understanding

List of Effective Pages

Section	Page No.	Revision	Date
List of Effective Pages	3	Original	2/4/98
Table of Contents	4	Original	2/4/98
Introduction	5	Original	2/4/98
Discussion - SecureID Card/Secure Modem Bank	5	Original	2/4/98
Discussion - Extension of the House Network	5	Original	2/4/98
Discussion - Vendor Internal Network Controls	6	Original	2/4/98
Discussion - Transmission Medium	6	Original	2/4/98
Discussion - Personnel Issues	6	Original	2/4/98
Discussion - House Network	6	Original	2/4/98
Discussion - Management, Audit, and Control	6	Original	2/4/98
Summary	7	Original	2/4/98
Attachment 1 – (MOU) HISFORM 015.0	Attachment	Original	2/4/98

Table of Contents

1.0 INTRODUCTION

Committee, Member, and other House office information systems currently face an environment of escalating integration complexity coupled with the need for fiscal constraint. In order 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 U.S. House of Representatives and the vendors themselves. The technical issues at hand, involve the methods by which vendors can remotely access the House network for performance of their support and maintenance actions.

2.0 DISCUSSION

A current method by which vendors perform remote support and maintenance is via the use of modems. This method of access is not secure and poses a significant threat to the integrity and security of the House network and the systems attached to the network. This lack of security was brought to light in the audit findings and recommendations published in the Inspector General/ PriceWaterhouse Audit report 95-CAO-01 dated May 3, 1995. Any future methods which permit vendors to remotely access House systems must first and foremost provide a high level of security. There are two methods that are endorsed to accommodate secure remote vendor access. One solution is suitable for limited, lower end support while the other provides for a high volume level of support. The two solutions are described as follows:

2.1 SecureID Card/Secure Modem Bank

To address the audit recommendation described above, an alternate secure access method is currently deployed. This method employs the use of SecureID (token) cards and a dedicated modem bank. While this solution is secure, it is better suited for casual, remote usage and limited (per session) vendor remote access due to its bandwidth limitations (up to 33.6 kbps). The SecureID token card provides the user with a “one-time” password via the token which is a credit card sized item with a digital, numeric display. The user enters a User ID and then a four digit PIN number and the six digit number that appears on the SecureID card for the password. The six digit number on the SecureID card is displayed for a period of one minute and then changes to another randomly selected number. The rationale for the security of this system is secure user authentication via two factors: (1) something the user *knows* (User ID and PIN) and (2) something the user *has* (token). Each SecureID card is synchronized in the system via the four digit PIN number and two entries of the randomly displayed six digit number. Successful authentication permits the user to obtain a network connection and use the services currently available on the House network with additional system and application ID and password entries as appropriate.

2.2 Extension of the House Network

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 for a connection of this nature are as follows:

2.2.1 Vendor Internal Network Controls

2.2.4.1 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.

2.2.4.2 All fileservers (including UNIX hosts) attached to the vendor's internal network are subject to the same secure configuration set up and audit controls as are enforced on House systems.

2.2.4.3 No Internet connections (or any other 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.

2.2.4.4 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 SecureID and modem bank method.

2.2.2 Transmission Medium

2.2.4.1 Direct connections to the House network must be via dedicated, point-to-point, non-switched telecommunication lines.

2.2.4.2 The vendor will assume all costs incurred for installation, termination, maintenance, and lease of the telecommunication line.

2.2.3 Personnel Issues

All vendor personnel involved in system support and maintenance of U.S. House of Representatives Information Systems including Committee, Member, and Officer offices, etc. are subject to the rules, regulations, and sanctions as outlined in: 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, and HISPOL 004.0 - U.S. House of Representatives Security Policy for Information System-Related Security Incidents.

2.2.4 House Network

2.2.4.1 CAO/HIR - Communications will provide and control the routed interface.

2.2.4.2 Vendor access to House information systems is limited to systems within their customer base only. Attempts to access systems outside the vendor's cognizance will be considered and handled as a breach of security.

2.2.4.3 Vendors shall not engage in any network monitoring or management activities without prior knowledge and approval of the Security Office.

2.2.5 Management, Audit, and Control

2.2.5.1 The vendor will 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.

2.2.5.2 The vendor's internal network will be subject to periodic audits and reviews conducted by CAO/HIR - Security personnel or their designees. These audits can include announced and unannounced: (1) on-site visits at the vendor facility to inspect the physical network plant, procedures, and controls, (2) network-oriented audits, and (3) office audits.

2.2.5.3 HIR Communications, Security Office, and vendor will be required to sign Attachment 1 - Memorandum of Understanding (MOU) - HISFORM 015.0, which will delineate each security control element of the telecommunication connection.

3.0 SUMMARY

The two methods of accessing House information systems described above provide vendors with better options on how to conduct the business of system maintenance and support. While both choices are technically secure, the human element will always be present as an "underlying" threat to system security. The types of access to House information systems required to properly perform administration, maintenance and support functions imply a significant burden of responsibility on vendor management and their personnel. The responsibilities include not only those associated with general system maintenance issues, but also the integrity and privacy of the information resident on these systems. For these reasons, the importance of a comprehensive audit and control program as implemented in this area cannot be overstated.