HISPOL 004.0

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

CATEGORY: **General Information Security**

ISSUE DATE: **February 4, 1998**
Revised Date: **August 23, 2000**

The United States House of Representatives
Committee on House Administration

Title: United States House of Representatives – Information Security Policy for Information System-Related Security Incidents

Number: HISPOL 004.0

Category: General Information 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 – **Information Security Policy for Information System-Related Security Incidents** is to provide users and contractor personnel with a policy regarding the handling and reporting of information system-related security incidents. The policy identifies the types of activity that constitute a system attack, the entity established to investigate and respond to such attacks, and security incident reporting.

Audience:

This document has relevance to all U.S. House of Representatives Members, Leadership Offices, Committees, employees, offices, contractors, and vendors who use House information system and network facilities.

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

Table of Contents

1.0 INTRODUCTION

The network-centric initiatives of CyberCongress will continue to result in an environment where open and expedient access to a wide range of information and services is made possible. As technology becomes more pervasive, systems become more vulnerable to attack from both inside and outside of the U.S. House of Representatives (House). Security policies and technological solutions have been and will continue to be enacted to provide protection for House information systems. The focus of these protections include: (a) network perimeter solutions for mitigating the threat of attack from external sources, and (b) host-based solutions for minimizing external and internal threats. Because all types of attacks are escalating in their level of sophistication, information systems security within the House will continue to be a top priority.

The new systems and capabilities are also coupled with an increase in individual responsibilities relative to the security of these systems. At the core of these responsibilities is the need for all House employees to respect and protect system resources and the privacy of information resident on all systems connected to the House network, including systems within Committee, Leadership, Member and other House Offices.

The purpose of this policy is to: (1) define an information security compliance and enforcement structure, (2) convey to all House employees the types of activities that could be considered intrusive and subject to disciplinary actions, and (3) outline the reporting structure.

2.0 TYPES OF INTRUSIVE ACTIVITY

The following is a list of intrusive activities that apply to both internal and external system attacks. The list includes but is not limited to:

- Attempts to intentionally gain access to, probe, or penetrate systems on which there is not an authorized account,

- Malicious or mischievous tampering (i.e., unauthorized viewing, modification, intentional introduction of malicious code/virus, deletion, etc.) of systems, data, and information resident on House systems,

- Unauthorized monitoring of aggregate network traffic for intelligence or information gathering purposes,

- Intentionally interfering with, shutting down, or impeding normal system operations,

- Using House information systems in a wasteful, fraudulent, or abusive manner,

- Abusing House information systems in a manner that could cause embarrassment to the U.S. House of Representatives,

- Theft or adverse modification of physical or intellectual property including copyright infringement,

- Any other actions that would circumvent House Rules, Federal law, or other security policies and procedures established for House information systems.

These types of activities will be pursued by authorities as serious matters and will not be tolerated in the U.S. House of Representatives. Some of these activities will be considered, at a minimum, unethical conduct while others could possibly violate Federal law. Depending on the nature and severity of the infraction, disciplinary actions may range from reprimand to dismissal and include criminal prosecution if deemed appropriate.

3.0 SECURITY INCIDENT INVESTIGATION AND RESPONSE

The Chief Administrative Officer has established the House Computer Incident Response Team (CIRT), an entity that responds to and investigates suspected and actual computer security activity as defined above. The CIRT operates under the management direction of the House Information Resources Information Systems Security Office. Members of the CIRT are representatives from each HIR Office and may include contractors and vendors as needed to resolve the specific incident under investigation.

4.0 SECURITY INCIDENT REPORTING

House network users need to be vigilant for unusual system behavior that may indicate a security incident has occurred. They should promptly report any suspected computer security incident to the Call Center or to the HIR Information Systems Security Office. Depending on the nature of the specific incident, user assistance may be required to efficiently resolve the incident. The process for reporting actual or suspected incidents is found in corresponding House Information Security Publications.

The House CIRT will generate a report regarding each House information system security incident. A database of security incidents will be maintained for reference purposes. All information regarding the investigation and resolution of security incidents will be considered Confidential House Information and shall be protected accordingly.

House CIRT management will report to the CAO and other House Officers and Committees as required. Coordination with outside authorities and reporting organizations will be conducted at the discretion of House CIRT and CAO management.

5.0 CONSEQUENCES OF NON-COMPLIANCE

Engaging in any activity considered intrusive in accordance with House Information Security Policies may subject the violator to appropriate disciplinary action including but not limited to the following:

- suspension of access privileges,
- warning (verbal or written),
- reprimand,
- suspension from employment,
- demotion from job position,
- termination of employment,
- financial liability for actual, consequential and incidental damages,
- criminal and civil penalties, including prison terms and fines.

The listed disciplinary actions are merely suggestions that can be used depending on the severity of the violation. This list is not exhaustive and does not imply that disciplinary actions are mandatory. It is within each employing authority's discretion to determine appropriate disciplinary measures under each circumstance. However, under the scope of House Rules and Committee on Standards of Official Conduct jurisdiction, certain violations may result in action by the House.