HISPOL 004.0

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

Version: 1.1
Approved: August 2006
Approved by: The United States House of Representatives Committee on House Administration

Table of Contents

1 Introduction

The network-centric initiatives of the United States House of Representatives (House) will continue to result in an environment where open and expedient access to a wide range of information and information services is made possible. As technology becomes more pervasive, information systems become more vulnerable to attack from both inside and outside the 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 safeguards includes network perimeter defense solutions mitigating the threat of attack from external sources, and host-based solutions that minimize external and internal threats. Because all types of attacks are escalating in their level of sophistication, information systems security within the House thrives and will continue to be a top priority.

As new information systems and capabilities grow, so do individual responsibilities relative to the security of these systems. At the core of these responsibilities is the need for all users of House information systems to respect and protect the privacy of information resident on all systems connected to the House enterprise network, including systems within Member, Committee, Leadership, and other House Offices.

1.1 Scope

The purpose of this policy is to identify the types of computer activities that could present a risk to the continued security of the House network, and to outline the reporting structure when such incidents occur.

2 Policy Guidelines

2.1 Types of Activity that Could Present a Security Risk to the Network

The following is a list of computer 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 House.
- 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 at the House. 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.

2.2 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 in *Section 2.1, Types of Intrusive Activity*. The CIRT operates under the management direction of the Information Systems Security Office (ISSO). Members of the CIRT are representatives from appropriate House Offices and may include contractors and vendors as needed to resolve the specific incident under investigation.

2.3 Security Incident Reporting

House information system users need to be vigilant for unusual system behavior that may indicate a security incident has occurred. They should promptly report any suspected information system or computer security incident to the Call Center, (202) 225-6002 / (800) 447-8737, or the ISSO, (202) 226-4988. Depending on the nature of the incident, user assistance may be required to efficiently resolve the incident. The process for reporting actual or suspected incidents is found in corresponding House of Representatives Information Security Publications (HISPUBs).

The House CIRT shall 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 shall be considered House sensitive information and protected accordingly. When such information is confidential to a specific Member, Committee, or Support Office, it will be protected at all times and in all forms; disclosure will be strictly limited to authorized individuals.

House CIRT management shall report to the CAO and other House Officers and Committees as required. Coordination with outside authorities and reporting

organizations shall be conducted at the discretion of House CIRT and CAO management.