HISPOL 007.0

The United States House of Representatives Information Security Policy for the Information Security Compliance Program

Version:	**1.0**
Approved:	**August 2006**
Approval Authority:	**The United States House of Representatives Committee on House Administration**

Table of Contents

1 Introduction

Securing information systems is an effort built on the premise that information - in all forms and development phases - must be protected from unauthorized access, modification, disclosure, destruction, and denial of service, whether intentional or accidental. In order to protect information, the systems and applications that process, store, and transmit the information must be adequately protected. How one defines "adequately" depends on the sensitivity of the information, the degree of risk faced by the system/application, and the security controls and safeguards put in place to reduce that risk to an acceptable level.

The United States House of Representatives (House) Information Systems Security Program (ISSP) provides a strategy for ensuring adequate security is established and maintained throughout the system development life cycle (SDLC) for all House information systems. This policy complements the ISSP by presenting guidance on what constitutes adequate security in terms of minimum-security requirements, and describes how compliance with those requirements will be achieved and monitored.

Security requirements for House information systems differ based on the type of system. For the purposes of this policy, information systems are categorized as major or support applications, or network-aware devices. Major applications may consist of one software application or a combination of hardware and software that support a specific mission-related function. Support applications are those that will not cause significant degradation to House operations in the event of a failure or interruption of service. Network-aware devices include, but are not limited to wireless access points, servers, workstations, modems, printers, and multi-function devices that are capable of connecting to the House network. Throughout the remainder of this policy, a network-aware device is referred to as a "device" or "devices". Security requirements for the House network are established and maintained by the Information Systems Security Office in accordance with the ISSP.

1.1 Scope

This document has relevance to all House Offices and provides policy governing security and compliance requirements applicable to all major and support applications and devices.

2 Policy Guidelines

The following policy guidelines address security requirements for House major and support applications and devices:

- House major and support applications and devices shall be protected commensurate with the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, modification or destruction of information processed, stored, or transmitted.

- The sensitivity of each major and support application shall be determined based on the value of the information processed, stored, or transmitted, and the potential impact of the loss of confidentiality, integrity, or availability.
- All major and support applications and devices shall undergo certification prior to implementation to ensure that appropriate security controls and safeguards have been implemented and are functioning.
- Compliance reviews of major and support applications and devices will be conducted at least once every two (2) years, or when a significant change occurs, to ensure an appropriate level of security is maintained. At the discretion of the ISSO, more frequent compliance reviews may be conducted.
- An Application Manager shall be designated for each major and support application with responsibility for ensuring adequate security is implemented and maintained throughout the SDLC.
- A System Administrator shall be designated for each device with responsibility for ensuring adequate security is implemented and maintained throughout the SDLC.
- Security requirements and controls (in place and planned) for each major and support application shall be identified and documented in a System Security Plan (SSP). SSPs shall be updated annually, and shall include device-related security controls and documents as appropriate.
- Security requirements and controls for each device shall be identified and documented in the appropriate security compliance checklist(s).

3 Roles and Responsibilities

Those with key roles in the successful implementation of this policy, and their associated responsibilities, are described below.

3.1 Information Systems Security Office

The Information Systems Security Office (ISSO) provides oversight and guidance regarding the security of all House major and support applications and devices. The ISSO will:

- Assess the adequacy, and coordinate the implementation, of security controls and safeguards.
- Review and approve System Security Plans.
- Conduct certification and compliance reviews of information systems prior to implementation, when a significant system change occurs, and at least once every two (2) years, and grant certification to operate based on the results of the security review.

- Provide security planning and risk management guidance and assistance to Application Managers and System Administrators.
- Ensure affected personnel receive appropriate security training in accordance with their responsibilities.
- Establish, implement, and maintain appropriate security controls and safeguards on the House network.

3.2 Responsible House Offices and Personnel

House Offices are responsible for the overall procurement, development, integration, modification, operation, maintenance, and oversight of an information system. The responsible personnel will:

- Ensure an Application Manager is designated for each major and support application and designate a Systems Administrator with operational security responsibility if the system is a device.
- Ensure a SSP is developed and maintained for each major and support application.
- Ensure the appropriate security compliance checklists are applied and maintained for devices.
- Ensure the major or support application or device is deployed and operated according to agreed-upon security requirements.
- Ensure users and support personnel receive appropriate security instruction.
- Determine the sensitivity of information processed by, and ensure a risk assessment is conducted for each major application, and for each support application as appropriate.
- Implement appropriate controls for the generation, collection, processing, dissemination, and disposal of information.

3.3 System Administrator

System Administrator roles are assigned to each device and are responsible for ensuring the appropriate operational security posture for each asset is maintained. The System Administrator will:

- Serve as the ISSO’s primary point of contact for all matters related to security.
- Apply the appropriate security compliance checklist(s) for the device as part of the certification and compliance review process.
- Comply with applicable policy requirements, such as those regarding Internet/Intranet access, server security, and wireless network security.

- Work with the ISSO to resolve security deficiencies and issues identified during initial certification, a compliance review, or as the result of an external audit (e.g., Inspector General audit).

3.4 Application Manager

The responsible House Office appoints an Application Manager for each major or support application. The Application Manager is responsible for ensuring the appropriate operational security posture for the application is maintained and will:

- Serve as the ISSO's primary point of contact for all matters related to security.
- Develop and annually update the SSP.
- Identify and implement appropriate security requirements and controls, and ensure adequate security is maintained throughout the SDLC.
- Inform the ISSO whenever a substantial change occurs in the major or support application.
- Participate in conducting a risk assessment prior to implementation, and at least once every two (2) years thereafter, as part of the compliance review process.
- Work with the ISSO to resolve security deficiencies and issues identified during initial certification, a compliance review, or as the result of an external audit (e.g., Inspector General audit).

4 Certification

Certification is the process of assessing security controls in an information system to determine the extent to which the controls are correctly implemented, operating as intended, and producing the required outcome with respect to meeting the protection requirements. Certification supports the risk management process by providing important information necessary to make credible, risk-based decisions on whether to place a major or support application or device into operation or to continue their current operation.

The certification process for applications and devices is described below. They shall be certified prior to their initial implementation, and the process shall be repeated in the form of a compliance review whenever a significant system change occurs, or at least once every two (2) years. Certification and compliance reviews shall be conducted by the ISSO, and shall culminate in the issuance of a Security Certification.

4.1 Major applications

A major application may consist of one (1) major software application or a combination of hardware and software that support a specific mission-related function. Thus, a major application may be supported by a number of servers running various operating systems and software applications that together accomplish a particular function. Such major applications must focus not only on protecting the information contained within the application itself, but on the devices that store, process, and transmit it as well.

The level of effort applied to the compliance review process for a major application shall be commensurate with the sensitivity of the application and its associated risk (i.e., the level of effort increases as the potential impact on operations, assets, or individuals increases).

Certification of a major application shall be based on:

- A risk assessment identifying:
    - threats and vulnerabilities
    - the potential impact and magnitude of harm to operations, assets, or individuals that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information system, and
    - the effectiveness of current or proposed security controls.
- A review of the application's SSP.
- A review of the sensitivity of the application.

Any security deficiencies found or issues identified shall be corrected or sufficiently addressed prior to certification.

4.2 Support applications

A support application is an information system that will not cause significant degradation to House operations in the event of a failure or interruption of service. This type of application may be supported by one or more servers running various operating systems. Such an application must focus not only on protecting the information contained within the information system itself, but on the devices that store, process, and transmit it as well.

The level of effort applied to the compliance review process for a support application shall be commensurate with the sensitivity of the application and its associated risk (i.e., the level of effort increases as the potential impact on operations, assets, or individuals increases).

Certification of a support application shall be based on:

- A review of the application's SSP.
- A review of the sensitivity of the application.
- If appropriate, a risk assessment identifying:
    - threats and vulnerabilities

  - the potential impact and magnitude of harm to operations, assets, or individuals that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information system, and
  - the effectiveness of current or proposed security controls.

Any security deficiencies found or issues identified shall be corrected or sufficiently addressed prior to certification.

4.3 Network-Aware Devices

Certification of devices shall be based on:

- Application and review of the appropriate security compliance checklist(s).
- Vulnerability assessment results.

High-risk devices (e.g., outward-facing servers), or those containing, processing, or transmitting highly sensitive data, will be subject to a more rigorous certification process and more frequent compliance reviews.

Any security deficiencies found or issues identified shall be corrected or sufficiently addressed prior to certification.

4.4 Enterprise-Wide Security Assessments

In addition to assessing major and support applications and devices, the ISSO conducts enterprise-wide security assessments of the House network. There are two (2) classes of enterprise-wide security assessments:

- Quarterly vulnerability assessments
- Immediate needs vulnerability assessments

Approximately once every three (3) months, the House network is assessed to determine if devices contain network-based vulnerabilities. Enterprise-wide assessments are designed to identify common vulnerabilities that pose significant risk to the House network yet, typically, require minimal effort to correct.

Immediate needs vulnerability assessments are conducted across the House network on an as-needed basis. These assessments are conducted when a software vendor releases a security bulletin concerning newly discovered, high-risk vulnerabilities that may exist on House devices. When technically possible, the ISSO will devise a method to inspect all House devices for the existence of this specific vulnerability.

4.5 Security Remediation Process

Vulnerabilities identified during the review process of a major or support application, device, or the House network are documented and tracked throughout the remediation process. Identified vulnerabilities are prioritized based on the risk each poses.

The level of risk each vulnerability poses is based on the sensitivity of the information processed and the type of access provided. In general, Internet-accessible devices and applications are given higher priority for remediation than those that are only accessible from the House internal network.

Once a vulnerability is identified, a corrective action is formulated and a timeframe established for its implementation. The ISSO will coordinate with the Systems Administrator or Application Manager to ensure corrective action has taken place. Upon completion, the ISSO will confirm the vulnerability has been mitigated.

For those vulnerabilities that have either no known corrective action or the implementation of a corrective action will seriously impair the functionality of the application, a risk acceptance plan will be formulated.

5 Minimum Security Controls

In accordance with government and industry best practices, the following minimum security controls are required. Additional security controls may be necessary depending on the sensitivity of the information processed and the potential risk and magnitude of harm that could result from the loss of confidentiality, integrity, or availability.

The minimum security controls presented in this section are required to appropriately protect House information. Security controls may be tailored as appropriate to reflect risk assessment results and must be documented.

5.1 Risk Assessment

Risks to the House network resulting from the operation of a device or major or support application should be identified. The risk assessment should include an inventory of devices, identification and assessment of threat sources and vulnerabilities, and an assessment of the effectiveness of current or proposed safeguards. Connections to other devices, major applications, remote access capabilities, and wireless capabilities should be addressed.

5.2 Security Certification

A Security Certification should be received from the ISSO prior to placing the device or major application into operation. If deficiencies exist, an explicit plan for corrective action should be in place and implemented and monitored.

5.3 Physical and Environmental Protection

Sensitive facilities and restricted areas should be identified and designated, and access to such areas should be controlled via keys, combinations, or other access devices as appropriate. Mechanisms should be in place to address the storage and handling of information, visitor access controls, natural disruption/disaster protection, failure of supporting utilities, fire protection, temperature and humidity controls, environmental control training, and equipment delivery and removal.

5.4 Identification and Authentication

Identification and authentication mechanisms must be implemented that include provisions for uniquely identifying and authenticating entities (i.e., users or processes acting on behalf of users). Access must be gained through the presentation of an individual identifier (e.g., login ID) and authenticator(s) (e.g., password). User authentication mechanisms must comply with House information security policies (HISPOLs).

5.5 Logical Access Controls

When technically feasible, access control mechanisms must be in place that restrict or authorize the activities of users. Access privileges must be restricted to the minimum required to perform job duties (least privilege), and critical functions should be divided among different individuals (separation of duties). Remote access must be appropriately restricted and controlled.

5.6 Audit Trails

Audit records must include sufficient information to establish what events occurred and who or what caused the event, and must be appropriately protected and reviewed.

5.7 Disaster Recovery

Regular backups of the entire file system should be made to facilitate recovery efforts should a compromise occur. Regular backups make it easier to determine the chronology and nature of an attack. Backup tapes must be stored in a secured fireproof container or off-site. Since an attack may not be immediately apparent, House Offices should retain two (2) system backups for at least six (6) months.