CYBERSECURITY
Policy Glossary

Helping you stay fully compliant with House IT security regulations

CAO
CHIEF ADMINISTRATIVE OFFICER

HISPOL	Policy Synopsis
HISPOL 1 - Structure and Organization (2006)	• HISPOL 1 outlines the development process for HISPOLs, HISPUBs, and HISFORMs. • Provides authorities for approval of HISPOLs, HISPUBs, and HISFORMs.
*HISPOL 2 - Protection from Unauthorized Use (2010)	• Outlines the responsible and secure use of House Information Systems. • Details who may access House systems and information. • Outlines appropriate hardware and software requirements and individual user training requirements.
HISPOL 3 - Connecting to the House Local Area Network (2010)	• Details requirements for connecting to the House Local Area Network. • Establishes user reporting of security incidents to HIR. • Establishes guidelines for how Member and Committee websites must be hosted.
HISPOL 4 - Information System Security (2010)	• Outlines activities that present a potential security risk to the House network. • Details security incident investigation and response procedure. • Outlines security incident reporting requirements.
*HISPOL 5 - Remote Access to House Network (2010)	• Details appropriate procedures for remotely accessing the House network - VPN use - SecurID token use • Outlines vendor requirements and responsibilities.
HISPOL 7 - Information System Compliance Program (2010)	• Outlines the security controls and technical standards for systems and applications on the House network. • Accompanied by over 40 individual HISPUBs that detail specific technical security and configuration guidance. (e.g. Windows 10, Linux RedHat)
HISPOL 8 - Enterprise Mobile and Portable Devices (2018)	• Details security requirements for enterprise mobile and portable devices connected to the House network. • Includes requirements for passwords/PINs. • Sets minimum device configuration standards. • Outlines individual user responsibilities for proper use of mobile devices connected to the House network.
HISPOL 9 - Password Protection (2014)	• Details password requirements for House systems and applications. • Establishes requirements for password complexity and frequency of change.
HISPOL 10 - Protection of Sensitive Information (2010)	• Details requirements for the handling of House sensitive information. • Outlines process for determining information sensitivity levels. • Provides guidance for the physical and electronic protection as well as the disposal of sensitive information.

Find out more: https://housenet.house.gov/cybersecurity/policies

HISPOL 11 - Guidelines for Working Remotely (2010)	• Outlines the information security responsibility of remote/teleworking users. • Requires two-factor authentication and VPN use to access the House network.
*HISPOL 12 - Security Awareness and Training (2015)	• Details the training requirements for all users accessing House systems or data. • Requires annual security awareness training for all users. • Requires role-based training for users with elevated privileges and accesses.
HISPOL 13 - Common Requirements for Network Access (2015)	• Details the activities performed to secure the House network and data by the CAO Office of Cybersecurity. • These include anti-virus scanning, secure configuration, vulnerability scanning, and intrusion detection and incident response. • Outlines requirements for individual system owners and offices.
HISPOL 14 - Secure Configuration Management Program (2015)	• Details the **Secure Configuration Management Program (SCMP)** implemented by CAO Office of Cybersecurity to assist in security configuration compliance for House systems and servers. • SCMP helps reduce vulnerabilities by assisting system owners with the compliance of security configurations to their systems. • Outlines individual system owner and office requirements.
HISPOL 15 - Interconnection & Data Sharing Program (2015)	• Outlines the requirements for properly documenting IT interconnections between House and external entities. • Requires the establishment of an MOU and NDA between the respective parties. • Details security requirements for managing interconnections.
*HISPOL 16 - Privileged Account Management (2015)	• Outlines the requirements for users with elevated privileges to House IT systems and information. • Establishes procedures for properly identifying individuals with a need for elevated privileges. • Establishes limits on the use of and number of privileged accounts per office. • Requires role-based training and adherence to the documented Rules of Behavior for privileged users. • Recommends background screening for individuals who will have privileged access. • Outlines vendor and shared resource responsibilities.
HISPOL 17 - Protecting House Data in the Cloud (2016)	• Establishes a framework for the protection of information stored or processed in cloud-based technologies. • Outlines the process for security and technical review of potential cloud technologies. • Establishes the Committee on House Administration (CHA) as the authorizing official for cloud solutions.
HISPOL 18 - Media Sanitization (in Draft Form)	• Provides standards for sanitizing media when it has reached its end of life phase, before the media is disposed of, transferred or re-used. • Device sanitization is not required before destruction, if the device is encrypted. • Media transfers in District Offices are managed very differently than in the DC office. • This policy does not apply to data that remains on media that a Member chooses to take custody of when they leave the House at the end of his/her term.
HISPOL 19 - Active Directory (2018)	• AD is a directory service that allows for centralized management of user accounts, security, and resources. • Details requirements for creation and management of new AD accounts. • Outlines individual responsibilities for domain and office systems administrators.

CYBERSECURITY

HISPUB Glossary

Technical oversight for the implementation of House Information Security Publications

CAO
CHIEF ADMINISTRATIVE OFFICER

HISPUB	Publication Synopsis
HISPUB 02.1 – Communications Infrastructure Security (2006)	• Outlines security requirements for the House communications infrastructure assuring the continued security of the network and data. • Security Requirement checklists for: - Capnet Routers - Campus Routers - C5K Catalyst - Campus LS1010 ATM Switches
HISPUB 02.2 – Guidelines for the Secure Use of Digital Printers and Copiers (2006)	• Outlines recommendations for securing network-enabled digital printers, copiers, and multifunction devices installed throughout the House environment. • Considered as minimum recommended requirements. • Subject to change with regard to the identification of any new system anomalies or vulnerabilities.
HISPUB 02.3 – Committee and Event Room Security Standards (2006)	• Provides security standards for committee and event rooms specifically wiring and cabling standards. • Includes all House Offices and employees, contractors, and vendors.
HISPUB 02.5 – NetIQ Alerting Systems Overview (2011)	• Outlines an alerting system which emails designated personnel when an action was performed on any object within the Organizational Unit (OU). • Includes a Table of Events listing situations to be reported.
HISPUB 02.6 – Acceptable Use of the Guest Virtual Local Area Network (2007)	• Details guidelines for the acceptable use of the House Guest Virtual Local Area Network (VLAN). • Includes illustrated instructions to access the internet through the Guest VLAN.
HISPUB 03.1 – Guidelines for Connecting to the House Local Area Network (2006)	• Provides all users of HIR with procedures for permanent connections to the local area network (LAN), internet, and intranet security. • Includes the guidelines which must be fulfilled prior to connecting to the House LAN.

Find out more: https://housenet.house.gov/cybersecurity/policies

HISPUB 04.1 – Computer Incident Response Team Handbook (2012)	• Describes the creation of the Computer Incident Response Team (CIRT) by the House CAO Information Security Office to preserve the availability, confidentiality, and integrity of information available on the House network. • Includes CIRT organization, operating procedures, roles, and responsibilities.
HISPUB 05.1 – SecurID Guidelines (2018)	• Provides guidance for remote access devices to the House network. • Relevant to all Member, Committee, and Leadership Offices, staff, contractors, and vendors that utilize SecurID.
HISPUB 06.1 – Wireless Network Security Best Practices (2010)	• Provides a basic overview of wireless and wireless security technologies and guidance for the secure operation of wireless devices. • Includes additional security information on WLANs, VPNs, and VLANs.
HISPUB 07.1 – Information Systems Security Certification Process for Network-Aware Devices (2011)	• Outlines security, audit, and certification roles for all network-aware devices that connect to the House network in accordance with House Information Security Policies and Publications.
HISPUB 08.1 – Best Practices for Wireless Handheld Devices (2006)	• Provides the House user community with guidelines for using, implementing, and administering wireless handheld devices.
HISPUB 10.1 – Guidelines for Determining Information Sensitivity and Security Categorization (2006)	• Questionnaire for assignment of impact levels and security categorization. • If the answer to any question in any category is “yes,” the information is considered sensitive and must be protected accordingly.
HISPUB 14.1 – Remote Access Software List (2017)	• The Office of Cybersecurity blocks applications that are considered “high risks”, especially those allowing remote access connectivity. • Third-Party Remote Desktop Software currently allowed: - Bomgar - Skype for Business - Native Operating System Remote Desktop Tools - Cisco AnyConnect (VPN Client)
HISPUB 15.1 – Information System Interconnection and Data Sharing Program Requirements (2015)	• Provides all users and owners of House information systems with guidance governing system interconnections with external information systems. • Relevant to all House Offices, employees, and contractors that connect to the House network.
HISPUB 18.03 – Quality Assurance (QA) Process (2017)	• Details the Director of Information Security’s (InfoSec) responsibility to enforce the QA process in accordance with HISPOL 18 – Electronic Media Sanitation.