National Institutes of Health (NIH)

Office of the Director (OD)

Office of the Chief Information Officer (OCIO)

Information Security and Awareness Office (ISAO)

6555 Rock Spring Drive
Bethesda, MD 20817

NIH Information Technology (IT) General Rules of Behavior

Version 2.0
April 9, 2019

RECORD OF DOCUMENT CONTROL

This NIH IT General Rules of Behavior may be updated as required to reflect regulatory, policy, standards, and organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed every three (3) years by the NIH Information Security and Awareness Office (NIH/OD/OCIO/ISAO) to ensure the NIH IT General Rules of Behavior remains relevant and accurate. Reviews and assessments made as part of this process are also included in the matrix below. This document history shall be maintained throughout the life cycle of this document.

Version	Release Date	Summary of Changes	Section(s) Updated	Changes Approved By
1.0	04/13/2018	• Original Version.	All	NIH/OD/OCIO/NIH InfoSec Program
2.0	04/09/2019	• Updated to align with July 2018 version of HHS General Rules of Behavior. • Included prohibition of the use of HHS e-mail address to create personal commercial accounts. • Integrated rules for personal use of government IT resources. • Restated some of the HHS rules into plain language to improve readability. • Added additional topic headings for clarity and realigned rules accordingly. • Added general staff policy requirements from NIH Information Security Manual Chapters pertaining to remote access, use of government furnished equipment, PIV card authentication, mandatory training, and mobile devices. This was done to enhance visibility of these requirements.	All	NIH/OD/OCIO/NIH InfoSec Program

Table of Contents

1 Introduction

1.1 Purpose

The National Institutes of Health (NIH), Office of the Director (OD), Office of the Chief Information Officer (OCIO), Information Security and Awareness Office (ISAO) provides oversight for the NIH IT General Rules of Behavior, which provides direction to NIH and the Institutes and Centers (ICs) for appropriate use of NIH information systems and resources for all employees, contractors, and other personnel who have access to NIH information and information systems.

The NIH IT General Rules of Behavior supplements the Department of Health and Human Services (HHS), Office of the Chief Information Officer (OCIO), HHS Rules of Behavior for Use of HHS Information and IT Resources Policy, which provides direction for appropriate use of HHS/OpDiv information systems and resources for all employees, contractors, and other personnel who have access to HHS information and information systems.

This NIH IT General Rules of Behavior supersedes previous versions of this document. This document does not supersede any other applicable law or higher-level HHS policies, directives, memorandum, or standards. All references noted in this document are subject to periodic revision, update, and reissuance.

1.2 Scope

This NIH IT General Rules of Behavior applies to all ICs, and all personnel conducting business for, and on behalf of, NIH, whether directly or through contractual relationships. This document does not supersede any other applicable law, higher level HHS or NIH directives, or existing labor management agreements in place as of the effective date of the NIH IT General Rules of Behavior.

NIH officials must apply the NIH IT General Rules of Behavior to employees, contractor personnel, interns, fellows, guests, and other non-government employees conducting business for the NIH, or on its behalf through contractual relationships or memoranda of agreement, when using HHS or NIH information systems or resources. All organizations collecting or maintaining information or using or operating information systems on behalf of the NIH, are also subject to the stipulations of the NIH IT General Rules of Behavior.

The NIH IT General Rules of Behavior shall apply to all users of NIH information and IT resources whether working at their primary duty station, while teleworking, at a satellite site or any other alternative workplaces, and while traveling.

1.3 References and Attribution

The following laws, regulations, policies, standards, and guidelines were used to provide the content for and compile this document:

- Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073, codified at 44 U.S.C. Chapter 35, Subchapter II, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

- 5 U.S.C. Section 552a (the Privacy Act), https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.
- NIST SP 800-88, *Guidelines for Media Sanitization,* December 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.
- NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf.
- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
- National Institute of Standards and Technology (NIST) White Paper, *Best Practices for Privileged User PIV Authentication,* April 21, 2016, http://csrc.nist.gov/publications/papers/2016/best-practices-privileged-user-piv-authentication.pdf.
- Office of Management and Budget (OMB), Circular A-130, Managing Information as a Strategic Resource, July 2016, https://www.whitehouse.gov/omb/information-for-agencies/circulars.
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf.
- OMB M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-05.pdf.
- OMB M-17-09, Management of High Value Assets, https://www.whitehouse.gov/omb/information-for-agencies/memoranda.
- OMB M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, October 2015, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-03.pdf.
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, as amended, https://www.whitehouse.gov/omb/information-for-agencies/circulars.
- HHS Information Security and Privacy Policy (IS2P) - 2014 Edition, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- HHS Policy and Plan for Preparing for and Responding to a Breach of PII, June 29, 2017.
- HHS Standard for Encryption of Computing Devices and Information, December 14,

2016, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.

- HHS Memorandum for Use of GFE during Foreign Travel, December 9, 2016, https://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- HHS Memorandum for the Updated Departmental Standard for the Definition of Sensitive Information, May 18, 2009, http://intranet.hhs.gov/it/cybersecurity/policies/index.html.
- Usage of Unauthorized External Information Systems to Conduct Department Business, January 8, 2014
- HHS Waiver/Risk Acceptance Form, retrievable from: https://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/Waiver/hhs_policy_waiver_20110729.pdf.
- NIH Information Security Policy Handbook
- NIH Information Security Incident Response Plan
- NIH Mobile Device Security Policy
- NIH Mobile Device Security Standard
- NIH Policy Manual Chapters:
    - 1405 - NIH Physical Access Control
    - 1440 - Dissemination of Security and Intelligence-Related Information
    - 1745 - NIH Information Technology (IT) Privacy Program
    - 1745-1 - NIH Privacy Impact Assessments
    - 1745-2 - NIH Privacy and Information Security Incident and Breach Response Policy
    - 1750 - NIH Risk Management Program
    - 1825 - Information Collection from The Public
    - 2801 - Access Control Facilities on Mainframe Computers
    - 2804 - Public-facing Web Management Policy
    - 2805 - NIH Web Privacy Policy
    - 2810 - NIH Remote Access Policy
    - 2811 - NIH Policy on Smart Card Authentication
    - 2813 - NIH Information Security and Privacy Awareness Training Policy
    - 2814 - NIH Policy on the Prohibited Use of Non-Government Furnished (Non-GFE) IT Equipment
    - 2815 - NIH Policy on the Use of Peer-to-Peer Software
    - 2817 - NIH Policy for Special Computer Monitoring of Employee Use of Information Technology (IT)
- NIH Wireless Network Security Policy
- NIH Wireless Network Security Standard

1.4 Document Effective Date

The effective date of the NIH IT General Rules of Behavior is ninety (90) days after the issuance. All NIH ICs and Offices shall implement the NIH IT General Rules of Behavior within ninety (90) days from issuance date.

1.5 Document Review

At a minimum, this document will be reviewed and assessed every three (3) years by the NIH Information Security and Awareness Office (NIH/OD/OCIO/ISAO) to ensure the NIH IT

General Rules of Behavior remains relevant and accurate. The details associated with this these reviews and updates are captured on the Record of Document Control page.

1.6 Assistance

Please direct any questions, comments, suggestions, or requests for further information to the NIH InfoSec Program at NIHInfoSec@nih.gov or 301-881-9726.

2 NIH IT General Rules of Behavior

2.1 General

- Obey federal laws, regulations, and NIH policies, standards, and procedures, and never direct or encourage others to violate them.
- Do not allow unauthorized use or access to NIH information, information systems and IT resources.
- Never bypass security safeguards (e.g., security and privacy policies, systems configurations, or access control procedures), unless your supervisor has given written authorization.
- Conduct yourself professionally in the workplace and be accountable for your actions.

2.2 Equipment

- Government furnished equipment (GFE) includes all IT equipment furnished by the government, and with regard to these rules, contractor furnished equipment (which is governed by the requirements set forth in the HHS Security and Privacy Language for Information and Information Technology Procurements.
- Only GFE can be used to perform official duties or to connect to NIH IT resources (excluding NIH public websites and other public use systems).
- Do not physically connect personally-owned IT equipment such as flash drives, external hard drives, mobile devices to GFE.
- Never allow others to use your GFE and/or other NIH IT resources that are provided to you to perform your official work duties.
- Official authorization is required to reconfigure systems, modify GFE, install/load unauthorized/unlicensed software or make configuration changes.
- Properly secure all GFE (including laptops, mobile devices, and other equipment that store, process, and handle NIH information) when leaving them unattended either at the office and other work locations, such as home, hoteling space, etc. and while on travel. This includes locking workstations, laptops, placing GFE in a locked drawer, cabinet, or simply out of plain sight, and removing your PIV card from your workstation.
- Contact your IC Information Systems Security Officer when planning to bring GFE and loaner equipment on foreign travel and follow your Institute/Center (IC) procedures.
- Review the HHS memorandum on the use of GFE during foreign travel and other HHS foreign travel requirements prior to traveling abroad with GFE or to conduct NIH business.
- The use of mobile devices (i.e., cell phones, smart phones, tablets) that wirelessly or physically connect to internal NIH IT resources, or synchronize with NIH enterprise services such as email, cloud-hosted file storage and collaboration sites must comply with the following:
    - Government furnished mobile devices must be enrolled in the approved enterprise-wide Mobile Device Management (MDM) service before being allowed direct access to NIH IT resources.
    - Personally-owned or contractor-furnished mobile devices may only access NIH IT resources through an application “container” managed by the approved enterprise-wide MDM service.

- Acceptance of the appropriate NIH Mobile Device Rules of Behavior and End User Agreement.
- Mobile devices used for official business must not be modified to circumvent the manufacturer's operation system security features or to circumvent the NIH configurations and security controls implemented as part of the MDM service.
- Mobile devices must be password or PIN protected. Enhanced authentication may be used for devices that have the functionality (e.g., biometrics).
- Lost or stolen mobile devices—both government-furnished and non-government furnished must be reported to the NIH IT Service Desk within one hour (60 minutes) so that the government information on the device can be remotely removed.

2.3 Accessing NIH Systems and Networks

- Personal Identity Verification (PIV) cards, Personal Identification Numbers (PIN), passwords and other access credentials must be protected from disclosure and compromise and never shared. Change passwords when required by NIH policy and/or if you suspect it's been compromised.
- Access to NIH IT systems and networks (including NIH-networked desktop and laptop computers) will only be granted by using PIV card authentication.[1]
- In cases where privileged access is needed (e.g. system, network or computer administrators), it must be granted through PIV card authentication to the maximum extent possible.
- Never use another person's account, identity, password/passcode/PIN, or PIV card.
- Only use authorized credentials, including PIV cards, to access NIH systems and facilities.
- Remote access to NIH IT resources requires use of a PIV card (or other approved NIH Smart Card or Secure ID token) and use of the NIH Virtual Private Network or other NIH approved remote access mechanism (e.g., CITRIX).
- Never connect GFE to unsecured Wi-Fi networks (e.g. airports, hotels, restaurants, etc.) or public Wi-Fi to conduct NIH business unless the Wi-Fi is at minimum password protected.

2.4 Data Protection

- Take all necessary precautions to protect NIH information and IT resources, including but not limited to hardware, software, sensitive information, federal records [media neutral], and other NIH information from unauthorized access, use, modification, destruction, theft, disclosure, loss, damage, or abuse, and in accordance with NIH information handling policies.

[1] Mechanisms that bypass PIV card authentication such as user ID/password are not allowed. Exceptions may only occur under the following conditions: 1) approved waiver from the NIH Chief Information Security Officer; 2) temporary access granted through the NIH IT Service Desk due to a forgotten, lost, or stolen PIV card; or 3) devices that cannot physically accept a PIV card that can authenticate through a PIV-derived credential.

- Protect sensitive information (e.g., personally identifiable information (PII)[2], protected health information (PHI)[3], confidential business information, financial records, proprietary data, etc.) stored on laptops or other computing devices, regardless of the media or format, from disclosure to unauthorized persons or groups by taking these actions:
    - Never store it in public folders, unauthorized devices/services or other unsecure physical or electronic locations.
    - Encrypt it when you're transmitting it via email, attachment, media, or other means.
    - Disseminate passwords and encryption keys out of band (e.g., via text message, in person, or phone call). When sending encrypted emails or transporting encrypted media, store the password and encryption keys separate from encrypted files, devices and data.
    - Only access or use it when necessary to perform job functions, and not for anything other than authorized purposes.
    - Securely dispose of electronic media and papers that contain sensitive data when no longer needed, in accordance with NIH records management and federal guidelines.
- Do not use personal email and storage/service accounts to conduct NIH business.
- Never use personal devices to conduct NIH business or store/transmit NIH data without official approval. Using personal phones to take phone calls or attend remote meetings is permitted.

2.5 Suspected and Identified Information Security Incidents

- Within one (1) hour of occurrence/discovery, notify the NIH IT Service Desk and the NIH Information Security Program to report:
    - All security incidents (e.g., actual or potential loss of control or compromises (whether intentional or unintentional, of your login name and password), PII and other sensitive NIH information maintained or in possession of NIH or information processed by contractors and third parties on behalf of NIH).
    - Emails that request NIH personal or organizational information or ask you to verify NIH accounts or security settings.
    - Lost or stolen NIH-issued equipment.

[2] PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Review other examples.

[3] PHI as defined in the HIPAA Privacy Rule, is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition;
- the provision of health care to the individual;
- the past, present, or future payment for the provision of health care to the individual; and/or
- an individual's information for which there is a reasonable basis to believe that it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g. name, address, birth date, Social Security Number).

2.6 Privacy

- Be aware that you should have no expectation of privacy when using or accessing NIH IT resources:
  - Your actions and activities are subject to NIH monitoring, recording, and auditing.
  - Use of GFE may not be secure, is not private, is not anonymous, and may be subject to disclosure under the Freedom of Information Act or other applicable legal authority.
  - Electronic data communications and online activity may be monitored and disclosed to external law enforcement agencies or NIH personnel when related to the performance of your duties. For example, after obtaining management approval, NIH authorized staff may employ monitoring tools in order to maximize the utilization of NIH resources.
- Do not access information about individuals unless specifically authorized and required as part of your assigned duties.
- Only collect information about individuals that is required by your assigned duties and authorized by a program-specific law, after complying with any applicable notice or other legal requirements[4].
- Only use information about individuals (including PII and PHI) for the purposes for which it was collected and consistent with conditions set forth in stated privacy notices such as those provided to individuals at the point of data collection or published in the *Federal Register* (to include System of Records Notices).
- Ensure the accuracy, relevance, timeliness, and completeness of information about individuals, as is reasonably necessary and to the extent possible, to assure fairness in making determinations about an individual.
- Only release information to members of the public (including individuals, organizations, the media, individual Members of Congress, etc.) as allowed by the scope of your duties, applicable HHS/NIH policies, and the law.
- Never use non-public NIH data for private gain or to misrepresent yourself or NIH or for any other unauthorized purpose.
- Do not maintain any record describing how an individual exercises his or her First Amendment rights, unless it is expressly authorized by statute or by the individual about whom the record is maintained or is pertinent to and within the scope of an authorized law enforcement activity.

2.7 Acceptance Personal Use of NIH IT Resources

- NIH allows you to have limited personal use of IT resources, including NIH email and instant messaging tools, systems and GFE (e.g., laptops, mobile devices, etc.) as long as the use:
  - Involves no more than minimal additional expense to NIH, does not disrupt your work productivity, interfere with the NIH mission or operations, or violate HHS/NIH security and privacy policies.

[4] Laws include, but are not limited to the Privacy Act of 1974, the Paperwork Reduction Act, and agency privacy policies and OMB memoranda, such as OMB Memorandum M-17-06 governing collection of PII on agency websites.

  - Does not adversely affect the security of NIH information, services, information systems, coworkers or cause network degradation (e.g., using social media, large amounts of storage space or bandwidth for personal reasons, such as digital photos, music, or video, using NIH email to create personal sites or subscribe to personal services and memberships, etc.).
- Except for the limited personal use stated above, refrain from using GFE, email, third-party website and applications, social media and networking sites (such as YouTube, Twitter, Facebook, etc.) or other NIH information resources for activities that are not related to any legitimate/officially-sanctioned NIH business purpose.

2.8 Internet and Email Use

- You may not access NIH Webmail from the public Internet.
- Do not click on links or open attachments sent via email or text message Web links from untrusted sources and verify information from trusted sources before clicking attachments.
- You may not auto-forward from an NIH email account.
- Do not provide personal or official NIH information to an unsolicited email.
- Only disseminate authorized NIH information related to your official job and duties at NIH to internal and external sources. Do not upload or disseminate information which is at odds with HHS/NIH missions or positions or without proper authorization because it could create the perception that the communication was made in your official capacity as a federal government employee or contractor.

2.9 Mandatory Training for NIH Information Security and Information Management[5]

- Use the NIH Information Security Training System to take and document courses.
- To be eligible to receive an NIH network account, complete:
  - Information Security Awareness for New Hires, and
  - Information Management for New Hires
- To keep this account, complete the annual NIH Information Security and Management Refresher.
- To be eligible for remote access privileges, complete the NIH Secure Remote Computing course (also requires approval from your IC management).
- Staff with significant security responsibilities must take annual training per HHS policy.

2.10 Strictly Prohibited Activities while using Federal Systems and Equipment

- Engaging in unethical or illegal conduct (e.g. pornography, criminal and terrorism activities, and other illegal actions and activities);
- Engaging in activities that could cause congestion, delay, or disruption of service to any NIH information resource (e.g., sending chain letters, playing streaming videos, games, music, etc.)

[5] Federal mandates for information security and privacy training include the *Federal Information Security Modernization Act*, the Office of Personnel Management Regulation, 5 CFR 930.301, the Department of Health and Human Services *Information Systems Security and Privacy Policy*, and the National Institute of Standards and Technology Special Publication 800-53, Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations.*

- Forwarding email spam, inappropriate messages, or unapproved newsletters and broadcast messages except when forwarding to report this activity to authorized recipients;
- Sending messages supporting or opposing partisan political activity as restricted under the Hatch Act and other federal laws and regulations.
- Engaging in outside fund-raising, endorsing any product or service, lobbying, or engaging in partisan political activity;
- Using peer-to-peer (P2P) software except for secure tools approved in writing by the NIH Chief Information Officer (or designee) to meet business or operational needs;
- Accessing, downloading and/or uploading illegal content from/to the Internet (e.g., pornographic and sexually explicit material, illegal weapons, terrorism activities and other illegal activities).
- Sending, retrieving, viewing, displaying, or printing sexually explicit, suggestive or pornographic text or images, or other offensive material (e.g. vulgar material, racially offensive material, etc.);
- Using NIH information, systems, devices and resources to:
    - Send or post threatening, harassing, intimidating, or abusive material about anyone in public or private messages or any forums;
    - Engage in activities that are inappropriate or offensive to fellow personnel or the public (e.g., hate speech or material that ridicules others on the basis of race, creed, religion, color, age, gender, disability, national origin, or sexual orientation;
- Creating and/or operating unapproved/unauthorized websites or services.
- Creating and/or uploading content to a website, third-party web application, or social media site on behalf of NIH without proper official authorization;[6]
- Using, storing, or distributing, unauthorized copyrighted or other intellectual property;
- Exceeding authorized access to sensitive information;
- Using NIH GFE to conduct or support commercial for-profit activities, managing outside employment or business activity, or running a personal business, shopping, instant messaging (for unauthorized and non-work-related purposes), playing games, gambling, watching movies, accessing unauthorized sites, and hacking;
- Using an official NIH email address to create personal commercial accounts for the purpose of receiving notifications (e.g., sales discounts, marketing, etc.), setting up a personal business or website, and signing up for personal memberships that are not work-related;
- Removing data or equipment from NIH premises without proper authorization;
- Sharing, transmitting, storing, processing, disclosing or processing sensitive NIH information using third-party organizations, systems, storage services or third-party applications (e.g., DropBox, Evernote, iCloud, etc.) unless authorized and with formal agreement in accordance with NIH policies.

[6] All third-party web applications, social media sites, storage and cloud services must be authorized prior to use and/or deployed into production by obtaining an authorization to operate (ATO) or included under an existing system's ATO. Consult your IC Information Systems Security Officer. In addition, you must be authorized to post authorized content on public-facing websites and social media sites.

- Transporting, transmitting, emailing, texting, remotely accessing, or downloading sensitive information unless such action is explicitly permitted in writing by the manager or owner of such information and appropriate safeguards are in place per NIH policies concerning sensitive information; and
- Knowingly or willingly concealing, removing, mutilating, obliterating, falsifying, or destroying NIH information.

2.11 Acknowledgement

I have read the above NIH General Rules of Behavior and understand and agree to comply with them.

- I understand that violations of these NIH Rules or information security policies and standards may result in disciplinary action, up to and including termination of employment; removal or debarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment.
- I understand that exceptions to these Rules must be authorized in advance in writing by the NIH Chief Information Officer or his/her designee.
- I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the NIH Rules draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Appendix A: Acronyms List

The following matrix contains a list of acronyms that may be in use across NIH. Some of the acronyms below may not be in this document, however, are provided to ensure the acronyms are expanded consistently across the enterprise.

Acronym	Full Term
Δ	Delta
A&A	Assessment and Authorization
ABAC	Attribute Based Access Control
AC	Access Control
AD	Active Directory
AF	Alternate Facility
AMS	Access Management Services
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
APEC	Asia-Pacific Economic Cooperation
APT	Advanced Persistent Threat
ARF	Asset Reporting Format
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
AV	Antivirus
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BIOS	Basic Input Output System
BLSR	Baseline Security Requirements
BPA	Blanket Purchase Agreement
BRM	Business Reference Model
BY	Budget Year
C&A	Certification and Accreditation
CA	Certificate Authority/Certificate Authorities
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCB	Configuration/Change Control Board
CCE	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIPS	Computer Crime and Intellectual Property Section
CCRB	Configuration Control Review Board
CCSS	Common Configuration Scoring System
CD	Compact Disk
CDM	Continuous Diagnostics Mitigation
CD-R	Compact Disk-Recordable
CEE	Common Event Expressions
CERIAS	Center for Education and Research in Information Assurance and Security
CERT/CC	CERT Coordination Center

Acronym	Full Term
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CFR	Code of Federal Regulations
CI	Configuration Item
CIKR	Critical Infrastructure And Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPSE	Confidential Information Protection and Statistical Efficiency Act
CIRC	Computer Incident Response Capability
CIRC	Computer Incident Response Center
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CIT	Center for Information Technology
CM	Configuration Management
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMS	Credential Management Services
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations
COPPA	Children's Online Privacy Protection Act
COTS	Commercial Off-The-Shelf
CP	Contingency Plan/Contingency Planning
CPE	Common Platform Enumeration
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CSF	Cybersecurity Framework
CSIRC	Computer Security Incident Response Capability
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSR	Center for Scientific Review
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CY	Current Year
DAA	Designated Approving Authority
DASD	Direct Access Storage Device
DB	Database
DBA	Database Administrator
DCS	Distributed Control System
DDoS	Distributed Denial of Service

Acronym	Full Term
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoD	Department of Defense
DoS	Denial of Service
DRM	Data and Information Reference Model
DRP	Disaster Recovery Plan
DS	Digital Signal
DVD	Digital Video Disc
DVD-R	Digital Video Disk-Recordable
DVD-ROM	Digital Video Disc - Read-Only Memory
DVD-RW	Digital Video Disc - Rewritable
EA	Enterprise Architecture
EAP	Employee Assistance Program
E-Auth	E-Authentication
EFS	External File Sharing
eGRC	Enterprise Governance Risk and Compliance
EMP	Electromagnetic Pulse
EMSEC	Emissions Security
EO	Executive Officer
EPLC	Enterprise Performance Life Cycle
EPP	Endpoint Protection Platform
ERA	E-Authentication Risk Assessment
ETA	E-Authentication Threshold Analysis
FAM	Financial Audit Manual
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configuration
FEA	Federal Enterprise Architecture
FEA SPP	Federal Enterprise Architecture Security and Privacy Profile
FedRAMP	Federal Risk and Authorization Management Program
FEMA	Federal Emergency Management Agency
FFMIA	Federal Financial Management Improvement Act
FIC	Fogarty International Center
FICAM	Federal Identity, Credential, and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
FIS	CIT Facility and Infrastructure Services
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act

Acronym	Full Term
FITSAF	Federal Information Technology Security Assessment Framework
FMFIA	Federal Managers Financial Integrity Act
FOIA	Freedom of Information Act
FPC	Federal Preparedness Circular
FS	Federation Services
FTE	Full-Time Equivalent
GAO	Government Accountability Office
GB	Gigabyte
GFIRST	Government Forum of Incident Response and Security Teams
GLB	Gramm-Leach-Bliley Act
GOTS	Government Off-the-Shelf
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GRC	Governance Risk and Compliance
GRS	General Record Schedule
GSA	General Services Administration
GSS	General Support System
HA	High Availability
HEW U.S.	Department of Health, Education, and Welfare
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVA	High Value Asset
HVAC	Heating, Ventilation, And Air Conditioning
HW	Hardware
I/O	Input/Output
IA	Information Assurance
IaaS	Infrastructure as a Service
IAM	Identity, Credential, and Assess Management Services
IANA	Internet Assigned Numbers Authority
IC	Institutes and Centers
ICS	Industrial Control System
ID	Identification
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IG	Inspector General
IIF	Information in Identifiable Form
IIHI	Individually Identifiable Health Information

Acronym	Full Term
IMS	Identity Management Services
InfoSec	NIH Information Security Program
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPA	Initial Privacy Assessment
IPSec	Internet Protocol Security
IR	Incident Response
IR	Interagency Report
IRB	Investment Review Board
IRC	Internet Relay Chat
IS	Information System
ISA	Interconnection Security Agreement
ISAC	Information Sharing and Analysis Center
ISC	Information System Component
ISC²	International Information Systems Security Certification Consortium
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
ISD	Instructional System Methodology
ISDN	Integrated Services Digital Network
ISO	Information System Owner or International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISOO	Information Security Oversight Office
ISP	Internet Service Provider
ISSE	Information System Security Engineer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISU	Information System User
IT	Information Technology
ITCP	Information Technology Contingency Plan
ITIL	Information Technology Infrastructure Library
ITL	Information Technology Laboratory
KSA	Knowledge, Skills, and Abilities
LACS	Logical Access Control System
LAN	Local Area Network
LCC	Life Cycle Cost
LDAP	Lightweight Directory Access Protocol
LSI	Large-Scale Integration
MA	Major Application
MAC	Media Access Control
MAO	Maximum Allowable Outage
MB	Megabyte
Mbps	Megabits Per Second
MEF	Mission Essential Functions

Acronym	Full Term
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSEL	Master Scenario Events List
MSSP	Managed Security Services Provider
MTD	Maximum Tolerable Downtime
MTTF	Mean Time To Failure
NARA	National Archives and Records Administration
NAS	Network-Attached Storage
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NC	Non-component
NCATS	National Center for Advancing Translational Sciences
NCCIC	National Cybersecurity and Communications Integration Center
NCCIH	National Center for Complementary and Integrative Health
NCI	National Cancer Institute
NDA	Non-Disclosure Agreement
NEF	National Essential Functions
NEI	National Eye Institute
NetBIOS	Network Basic Input/Output System
NFO	Nonfederal Organization
NHGRI	National Human Genome Research Institute
NHLBI	National Heart, Lung, and Blood Institute
NIA	National Institute on Aging
NIAAA	National Institute on Alcohol Abuse and Alcoholism
NIAID	National Institute of Allergy and Infectious Diseases
NIAMS	National Institute of Arthritis and Musculoskeletal and Skin Diseases
NIAP	National Information Assurance Partnership
NIBIB	National Institute of Biomedical Imaging and Bioengineering
NICHD	National Institute of Child Health and Human Development
NIDA	National Institute on Drug Abuse
NIDCD	National Institute on Deafness and Other Communication Disorders
NIDCR	National Institute of Dental and Craniofacial Research
NIDDK	National Institute of Diabetes and Digestive and Kidney Diseases
NIEHS	National Institute of Environmental Health Sciences
NIGMS	National Institute of General Medical Sciences
NIH	National Institutes of Health
NIH CC	NIH Clinical Center
NIMH	National Institute of Mental Health
NIMHD	National Institute on Minority Health and Health Disparities
NINDS	National Institute of Neurological Disorders and Stroke
NINR	National Institute of Nursing Research
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report

Acronym	Full Term
NKS	NIH Key Systems
NLM	National Library of Medicine
NOFORN	Not Releasable to Foreign Nationals
NPPI	Non-Public Personal Information
NSA	National Security Agency
NSAT	NIH Security Authorization Tool
NSP	Network Service Provider
NSPD	National Security Presidential Directive
NSRL	National Software Reference Library
NSTISSI	National Security Telecommunications and Information System Security Instruction
NTP	Network Time Protocol
NVD	National Vulnerability Database
NVD	National Vulnerability Database (formerly known as I-CAT)
OCI	Organizational Conflict of Interest
OCIL	Open Checklist Interactive Language
OCIO	Office of the Chief Information Officer
OD	NIH Office of the Director
ODNI	Office of the Director of National Intelligence
OECD	Organisation for Economic Co-operation and Development
OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OpDivs	Operating Divisions
OPM	Office of Personnel Management
OPSEC	Operations Security
ORS	Office of Research Services
OS	Operating System
OSOP	NIH Office of the Senior Official for Privacy
OT	Operations Technology
OVAL	Open Vulnerability and Assessment Language
P2P	Peer-to-Peer
PaaS	Platform as a Service
PACS	Physical Access Control System
PBX	Private Branch Exchange
PCIE	President's Council on Integrity and Efficiency
PDA	Personal Digital Assistant
PHI	Protected Health Information
PI	Pandemic Influenza
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	Personal Identification Verification Interoperable
PKI	Public Key Infrastructure

Acronym	Full Term
PL	Public Law
PMA	President's Management Agenda
PMEF	Primary Mission Essential Functions
PMP	Project Management Professional
POA&M or POA&Ms	Plan of Action and Milestones
POC	Point of Contact
PRA	Paperwork Reduction Act
PRISMA	Program Review for Information Security Management Assistance
PRM	Performance Reference Model
PTA	Privacy Threshold Analysis
PY	Prior Year
RAID	Redundant Array Of Independent Disks
RAR	Risk Assessment Report
RBAC	Role-Based Access Control
RD	Restricted Data
REN-ISAC	Research and Education Networking Information Sharing and Analysis Center
Rev.	Revision
RFC	Request for Comment
RFID	Radio-Frequency Identification
RID	Real-Time Inter-Network Defense
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA&A	Security Assessment & Authorization
SaaS	Software as a Service
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, Security
SAOP	Senior Agency Official for Privacy
SAP	Security Assessment Plan or Special Access Program
SAR	Security Assessment Report
SC	Security Category
SCA	Security Control Assessor
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCF	Security Control Families
SCI	Sensitive Compartmented Information
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SecCM	Security-Focused Configuration Management
SIA	Security Impact Analysis
SIEM	Security Information and Event Management

Acronym	Full Term
SISO	Senior Information Security Officer
SLA	Service-Level Agreement
SOA	Service-Oriented Architecture
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SOR	System of Records
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publication
SPP	Security and Privacy Profile
SRM	Service Component Reference Model
SSE	Systems Security Engineering - Capability Maturity Model®
SSH	Secure Shell
SSL	Secure Sockets Layer
SSN	Social Security Number
SSP	System Security Plan
ST&E	Security, Test, and Evaluation
StaffDivs	Staff Divisions
STIG	Security Technical Implementation Guidelines
SW	Software
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TERENA	Trans-European Research and Education Networking Association
TMIR	Threat Mitigation and Incident Response
TRM	Technical Reference Model
TT&E	Test, Training, and Exercise
U.S.	United States
U.S.C.	United States Code
UDP	User Datagram Protocol
UII	Unique Item Identifier
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USC	United States Code
US-CERT	United States Computer Emergency Readiness Team34
USGCB	United States Government Configuration Baseline
UTC	Coordinated Universal Time
UTSA	University of Texas-San Antonio
VLAN	Virtual Local Area Network
VM	Virtual Machine/Vulnerability Management
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTL	Virtual Tape Library
WAN	Wide Area Network

Acronym	Full Term
WiFi or Wi-Fi	Trademarked phrase (common name) for IEEE 802.11x
WLAN	Wireless Local Area Network
WORM	Write-Once, Read-Many
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

Appendix B: Rules of Behavior for Privileged Users

The following HHS Rules of Behavior (RoB) for Privileged Users is an addendum to the Rules of Behavior for General Users and provides mandatory rules on the appropriate use and handling of HHS information technology (IT) resources for all HH privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HHS information systems.[7] Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.[8] The compromise of a privileged user account may expose HHS to a high-level of risk; therefore, privileged user accounts require additional safeguards.

A Privileged User is a user who has been granted significantly elevated privileges for access to protected physical or logical resources. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity and availability. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include:

A. Application developer
B. Database administrator
C. Domain administrator
D. Data center operations personnel
E. IT tester/auditor
F. Helpdesk support and computer/system maintenance personnel
G. Network engineer
H. System administrator.[9]

Privileged users shall read, acknowledge, and adhere to the RoB for Privileged User and any other HHS policy or guidance for privileged users, prior to obtaining access and using HHS information and information systems and/or networks in a privileged role. The same signature acknowledgement process followed for the Appendix A, General RoB, applies to the privileged user accounts. Each OpDiv must maintain a list of privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account[10].

I understand that as a Privileged User, I must:

---

[7] Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, privileged roles include, for example, key management, network and system administration, database administration, and Web administration

[8] Office of Management and Budget (OMB), OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,* October 30, 2015.

[9] The definition is derived from the *Identity, Credential & Access Management (ICAM) Privileged User Instruction and Implementation Guidance*.

[10] Per National Institute of Standards and Technology (NIST) White Paper, *Best Practices for Privileged User PIV Authentication,* April 21, 2016

1. Use Privileged User accounts appropriately for their intended purpose and only when required for official administrative actions;
2. Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV)/ personal identified numbers (PINs) and other login credentials used to access HHS information systems;
3. Comply with all system/network administrator responsibilities in accordance with the HHS IS2P and any other applicable policies;
4. Notify system owners immediately when privileged access is no longer required;
5. Properly protect all sensitive information and securely dispose of information and GFE that are no longer needed in accordance with HHS/OpDiv sanitization policies;
6. Report all suspected or confirmed information security incidents (security and privacy) to the OpDiv Helpdesk and/or the OpDiv Security Incident Response Team (CSIRT) and my supervisor as appropriate; and
7. Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a Privileged User, I must not:

1. Share Privileged User account(s), password(s)/passcode(s)/PIV PINs and other login credentials;
2. Install, modify, or remove any system hardware or software without official written approval or unless it is part of my job duties;
3. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing;
4. Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment;
5. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes;
6. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into HHS information systems or networks;
7. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;
8. Use Privileged User account(s) for day-to-day communications and other non-privileged transactions and activities;
9. Elevate the privileges of any user without prior approval from the system owner;
10. Use privileged access to circumvent HHS policies or security controls;
11. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals;
12. Use a Privileged User account for Web access except in support of administrative related activities;
13. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner; and
14. Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS information:
    a. Antivirus software with the latest updates,
    b. Anti-spyware and personal firewalls,

c. A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access, and
d. Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

SIGNATURE

I have read the above Rules of Behavior (RoB) for Privileged Users and understand and agree to comply with the provisions stated herein. I understand that violations of these *RoB* or HHS information security policies and standards may result in disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to these *RoB* must be authorized in advance in writing by the designated authorizing official(s). I also understand that violation of federal laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which these RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

User's Name: _____
(Print)

User's Signature: _____

Date Signed: _____

Digital Signature (optional):

The record copy is maintained in accordance with General Records Schedule (GRS) 1, 18.a.

Appendix C: Minimum Set of HHS and NIH Roles Assigned Significant Responsibilities for Information Security

Both the Federal Information Security Management Act (FISMA) and the Office of Personnel Management (OPM) Regulation 5 Code of Federal Regulations (CFR) 930.301 require federal agencies to:

- Identify personnel with significant security responsibilities; and,
- Provide security training commensurate with these responsibilities in the form of role-based training.

Additionally, the requirements within this Handbook are consistent with the HHS IS2P. Within the HHS and NIH environments, significant security responsibilities are defined as the responsibilities associated with a given role or position, which, upon execution, could have the potential to adversely impact the security posture of one or more HHS or NIH systems. As such, the following roles, consistent with OPM Regulation 5 CFR 930.301 represent the *minimum* set of roles at HHS and NIH that possess significant security responsibilities. Each role is characterized by its population - both mandatory and optional members - and relevant responsibilities. These individuals include:

1. Executives

Mandatory Population:

- All members of the Senior Executive Service (SES).

Optional Population:

- None specified.

Relevant Responsibilities:

- Formulation of policy and guidance that may impact information system and/or security policy and operations.
- Allocation of resources to manage enterprise risk related to the use of information and information systems.

2. Chief Information Officers and Chief Information Security Officers

Mandatory Population:

- HHS CIO, direct managerial reports and component organizations, NIH and IC CIOs, direct managerial reports and component organizations, HHS CISO, and NIH and IC CISOs.

Optional Population:

- None specified.

Relevant Responsibilities:

- Establishment of information security and/or system policy.
- Management of the IT function and related risks.

3. IT Security Program Managers

Mandatory Population:

- Individuals with the titles of Information Systems Security Officer (ISSO), Information Security Officer (ISO), or System Security Officer (SSO) and their information security employees or contractors.
- All information security employees or contractors working for or contracted by the HHS CISO or the NIH CISO.

Optional Population:

- Positions within the GS-2210 Information Technology Management job series might fill this role.

Relevant Responsibilities:

- Implementation of information security policies.

4. Program and Functional Managers/Information Technology (IT) Functional Management and Operations Personnel

Mandatory Population:

- All personnel identified as a System Owner, Data Steward, Data Owner, Program Manager, or Project Manager.

Optional Population:

- Positions within the following series that might fill this role: GS-0332 Computer Operator, GS-0334 Computer Specialist, GS-2210 Information Technology Management, GS-0340 Program Management Series, and GS-0343, Management and Program Analysis.

Relevant Responsibilities:

- Stewardship of a system or its information assets during its development and/or operation.

5. IT Auditors

Mandatory Population:

- All personnel engaged in the auditing of HHS or NIH information technology systems or networks.

Optional Population:

- Positions within the GS-0511 Auditing job series might fill this role.

Relevant Responsibilities:

- Evaluation of systems for appropriate and effective implementation of controls to address security risks.

6. Other Security-Oriented Personnel

Mandatory Population:

- Information Technology (IT) administrators (e.g., network administrators, system administrators, and database administrators).

Optional Population:

- Positions within the GS-1550 Computer Science or the GS-0391 Telecommunications job series might fill this role.

Relevant Responsibilities:

- Enable the implementation and operation of one or more system security controls, as outlined in *NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations* (as amended).

NIH and ICs must identify employees and contractors who hold the aforementioned roles or responsibilities. The performance of this identification process is considered the completion of an NIH Personnel Needs Assessment. Personnel whose responsibilities are not captured within this appendix but meet the intent of the significant security responsibilities definition must also be designated. Personnel whose job duties meet these criteria must complete the HHS' RBT course(s) associated with their role. Personnel that assume multiple roles must complete training that addresses the unique risks associated with each role. However, this training may be combined at the NIH's discretion. HHS RBT courses can be located at http://intranet.hhs.gov/it/cybersecurity/training/role_based/index.html.

Alternatively, NIH may provide equivalent RBT to address the aforementioned roles, or combination of roles, with significant security responsibilities. Individuals beginning work with NIH or IC must be required to complete the appropriate RBT within three months of their initial start date.