LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

The Department of Health and Human Services
Information Security for IT Administrators

Information Security for IT Administrators

Introduction
Welcome to Information Security IT Administrators

Information Technology (IT) Administrators are the first line of defense in safeguarding information assets at the Department of Health and Human Services (HHS). This course will discuss your role in keeping IT systems secure throughout the life cycle and in daily operations.

At the end of the course, you will read and acknowledge the *HHS Rules of Behavior for Privileged User Accounts.*

References to HHS information security policies, standards, and guidance are provided for various course topics. Refer to your Operating Division's (OpDiv) security policies and procedures, in most cases they will be more specific than Department policy.

Introduction

Objectives

At the end of this course you will be able to:

❑ Understand your role and responsibilities to protect information security as an IT Administrator.

❑ Define the basic components of an information security program.

❑ Identify governing bodies and legislative drivers for protecting information systems.

❑ Understand the Enterprise Performance Life Cycle (EPLC) and Risk Management Framework (RMF) and how they relate to the development of IT systems.

❑ Understand the basics of responding to a security or privacy incident.

❑ Understand the basics of access control.

❑ Identify where to locate HHS policies, procedures, and guidance for securing IT assets.

Introduction
All It Takes is One Incident

▸ HHS' mission is protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.

▸ Sensitive health and personal information is collected and stored in HHS information systems to provide critical medical and social services to millions of people.

▸ Information security professionals are responsible for protecting the IT assets that support the mission from unofficial access, disruption of service, and unauthorized modification.

▸ Understanding the threats that information systems are exposed to and taking steps to mitigate them reduces the risk to networks and systems.
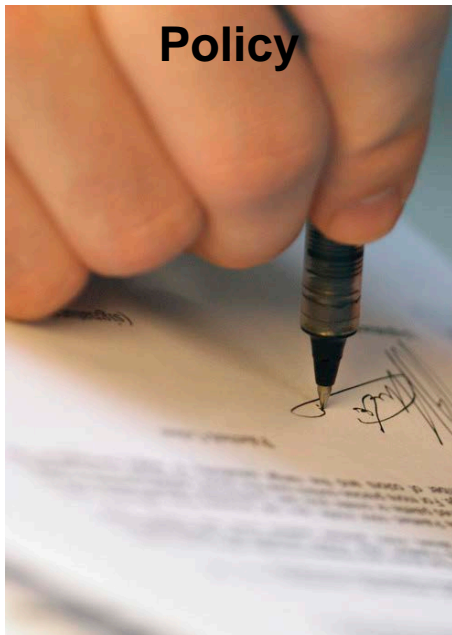
Safeguarding the HHS Mission
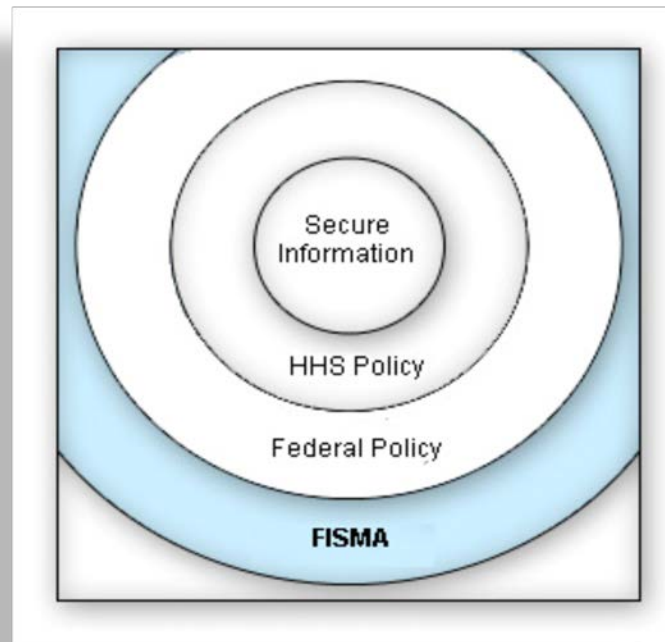
Safeguarding the HHS Mission
Security is an Integrated Solution

Information security is part of a complex interrelationship that includes policy, people, procedures, and products.

Policy

People

Procedure

Products

Safeguarding the HHS Mission
Policy

▸ The Federal Information Security Management Act (FISMA) is the backbone of federal legislation regarding information security. It requires federal agencies to develop, document, and implement an enterprise information security program to cost-effectively reduce IT security risks to federal information assets.

Safeguarding the HHS Mission
Department Governance

▸ The HHS Cybersecurity Program is the Department's information security program. Oversight is provided by the Office of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). The Program provides an enterprise-wide perspective, facilitating coordination among key stakeholders, setting standards and providing guidance to Operating Divisions (OpDivs), and supporting streamlined reporting and metrics capabilities.

▸ Operating Divisions manage implementation of Department standards, provide business/domain expertise, develop policies and procedures specific to the OpDiv's operating environment, and manage ongoing operations.

Safeguarding the HHS Mission
People

▸ Understanding the roles and responsibilities of the IT team members helps ensure communication and accountability.

▸ For a list of IT roles and responsibilities within HHS, please refer to the *HHS-OCIO Policy for Information Systems Security and Privacy*.

Safeguarding the HHS Mission
Procedure

Federal legislation and guidance influences the Department's technological infrastructure and information asset safeguards.

The table lists some sources of legislation and guidance that help to build an effective security program, thereby protecting information and systems.

IT Security Legislation and Guidance	Privacy Legislation	National Institute of Standards and Technology (NIST) Special Publications
▸ E-Government Act of 2002 ▸ Clinger-Cohen Act of 1996 ▸ Health Insurance Portability and Accountability Act of 1996 (HIPAA) ▸ Office of Management and Budget (OMB) Circular A-130	▸ Privacy Act of 1974 ▸ Paperwork Reduction Act ▸ Children's Online Privacy Protection Act (COPPA)	▸ NIST issues standards and guidelines to assist federal agencies in implementing security and privacy regulations. ▸ Special publications can be found on the Publications Portal.

Safeguarding the HHS Mission

Products

▸ Security must be considered when developing or acquiring any IT system.

▸ A system can involve anything from an off-the-shelf piece of software–or a hardware peripheral like a printer–to an enterprise-wide web-based application that is used daily by thousands of employees.

▸ All components–hardware, software, interconnections, facilities, infrastructure (e.g., power, temperature), etc.– are all part of the information system "product."

Information Security Program Management

Information Security Program Management
Introduction

▸ Individuals with hands-on responsibilities for the daily operations of systems must understand how their roles relate to the information security programs at the Department and OpDiv level.

▸ Such an understanding will enable IT Administrators to perform their duties with a mindset of appropriate and adequate protection for HHS' IT resources.

Information Security Program Management

Information Security Program Objectives

The overall objective of an information security program is to protect the information and systems that support the operations and assets of the agency.

▸ To safeguard each system at HHS is to ensure that the following security objectives can be realized for their information:

– **Confidentiality** - Protecting information from unauthorized access and disclosure.

– **Integrity** - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.

– **Availability** - Defending information systems and resources to ensure timely and reliable access and use of information.

Information Security Program Management

Threats

▸ Information systems are not perfect, nor are the people that interact with them or the environments in which they function. As such, systems are vulnerable to misuse, interruptions and manipulation.

▸ A threat is the potential to cause unauthorized disclosure, unavailability, changes, or destruction of an asset.

▸ Threats can come from inside or outside HHS.

  – External forces can disrupt a system, such as a hacker maliciously accessing or corrupting data, or a storm disrupting power and network access.

  – An example of an internal threat is an employee who inappropriately changes, deletes, or uses data.

Information Security Program Management
Vulnerability

▸ A vulnerability is any flaw or weakness that can be exploited and could result in a breach or a violation of a system's security policy.

▸ Some examples of vulnerabilities include:

– Poorly communicated or implemented policy;

– Inadequately trained personnel; and

– Improperly configured systems or controls.

Information Security Program Management

Risk

▸ A threat that exploits a vulnerability can allow information to be accessed, manipulated, deleted, or otherwise affected by those without the proper authority. It may also prevent data or a system from being accessed.

▸ Risk is the likelihood that a threat will exploit a vulnerability. For example, a system without a backup power source is a vulnerability. A threat, such as a thunderstorm, would increase the likelihood of a power outage and create a risk of system failure.

▸ Risk management is the process of identifying threats and vulnerabilities to IT assets and establishing acceptable controls to reduce the likelihood of a security breach or violation.

Information Security Program Management

Security Controls

No information system is completely safe from threats, but **controls** help mitigate risks.

▸ Controls are policies, procedures, and practices designed to decrease the likelihood, manage the impact, or minimize the effect of a threat exploiting a vulnerability. Examples of controls include:

- Clearly documented roles and responsibilities;

- Security awareness and training program;

- Incident response planning;

- Physical security, like guards, badges, and fences;

- Environmental controls in server rooms; and

- Access controls, like passwords and PINs.

Information Security Program Management
Annual Assessment

▸ Under FISMA, HHS must determine the effectiveness of its information security program.

▸ The Office of the Inspector General (OIG) annually audits information security policies and procedures.

▸ IT Administrators may be asked to help review existing security documentation, configurations, procedures, system testing, inventory, or anything else related to information security.
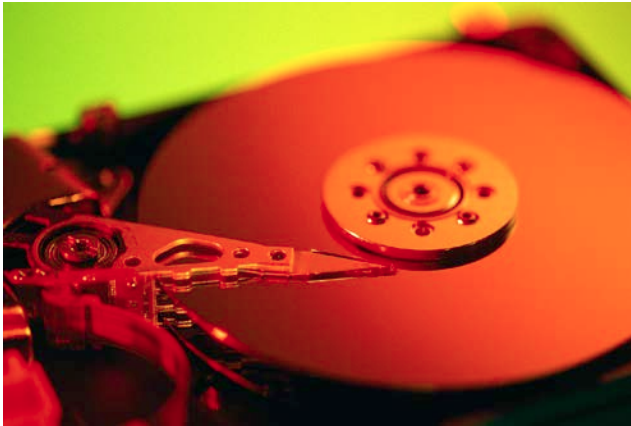
Information Security Program Management
Recap

▸ The goal of the information security program is to keep information and information systems appropriately confidential and available, while maintaining integrity.

▸ The likelihood and impact of a threat exploiting a vulnerability is a risk to the system.

– Example: Account privileges are not disabled when employees are terminated (vulnerability). A disgruntled former employee (threat) creates a risk that the organization's network and data will be compromised.

▸ There is an inherent risk in operating any information system. Controls help minimize and avoid some of the risk.

SYSTEM ACCESS
THREATS
VULNERABILITIES
LIKELIHOOD
IMPACT
CONTINGENCY
CRITICALITY
RISK LEVEL
CONTROLS

Enterprise Performance Life Cycle

Enterprise Performance Life Cycle

Introduction

▸ The EPLC is a standardized project management methodology that guides HHS IT investments and ensures that mission objectives are being met throughout the lifetime of a system.

▸ Security is essential to developing or deploying a successful IT system. Information technology administrators, like yourself, should be part of the EPLC from the beginning.

▸ A detailed explanation of the EPLC can be found in the Enterprise Performance Life Cycle Framework Overview Document.
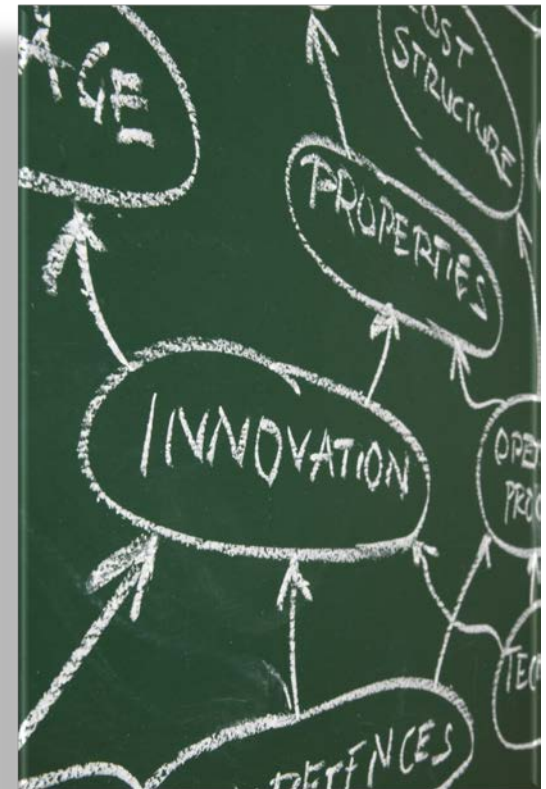
Enterprise Performance Life Cycle
Stakeholders

▸ Stakeholders are an essential piece of the EPLC puzzle. There can be many stakeholders depending on the size and scope of the project. In general, every project will include:

– Project Managers responsible for planning, executing and overseeing phase activities. They also are responsible for creating the deliverables for review in conjunction with the Critical Partners.

– Critical Partners responsible for reviewing the project deliverables and validating policies in their functional areas.

– IT Governance Organizations approve projects and monitor baselines and performance metrics throughout the life cycle. They also approve projects to advance to the next phase based on the recommendations of the Critical Partners.

Enterprise Performance Life Cycle
Deliverables

▸ The EPLC Framework Overview describes the documents and artifacts that need to be developed in each phase of the life cycle.

▸ Tailoring may reduce the level of effort and artifacts required for the phases. Changes to required documentation are identified in the Tailoring Agreement.

▸ For security documentation, at a minimum each system must have a System Security Plan (SSP), Risk Assessment, and Authorization to Operate (ATO).

▸ Documentation needs to be maintained throughout the life cycle of a system and should be stored accordingly.

Enterprise Performance Life Cycle
Recap

▸ The EPLC is HHS' IT project management methodology.

▸ The EPLC ensures that IT systems meet business and mission objectives, are well managed, and cost-effective from inception to disposal.

▸ Building security into a system early in the design process is far more efficient than trying to add it during or after development.

▸ Security Critical Partners ensure that security and privacy concerns are addressed during each phase of the life cycle.
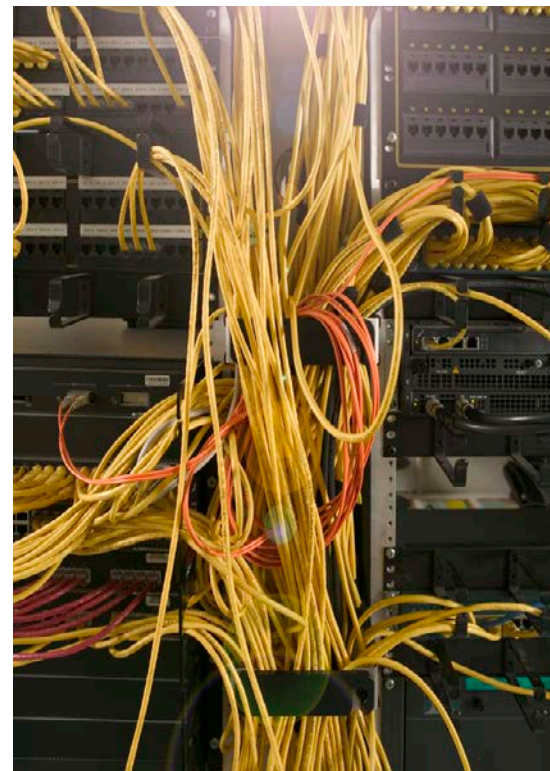
EPLC and the Risk Management Framework

EPLC and the Risk Management Framework
Introduction

▸ The RMF, as described in NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems, establishes a common risk management framework for all federal agencies to improve security and strengthen risk management processes.

▸ The RMF is a formal process used by HHS to ensure that security activities and artifacts are developed for all systems and applications at the right time.

EPLC and the Risk Management Framework

Risk Management Framework

At HHS, the RMF helps:

▸ Develop secure and compliant systems in a cost effective manner.

▸ Integrate security practices throughout the EPLC.

▸ Communicate security concepts and create a general understanding of security requirements.

▸ Provide support to project managers by helping them understand and comply with security requirements.

Categorize
the system

Select
the controls

Monitor
the system

Risk
Management
Framework

Implement
the controls

Authorize
the system

Assess
the controls

Source: NIST SP 800-37 Rev.1

EPLC and the Risk Management Framework
EPLC and RMF Integration

▸ The RMF is integrated into the EPLC so that IT security best practices and standards are built into a project from the beginning.

▸ The image below shows how the six steps of RMF are merged across the ten phases of EPLC.
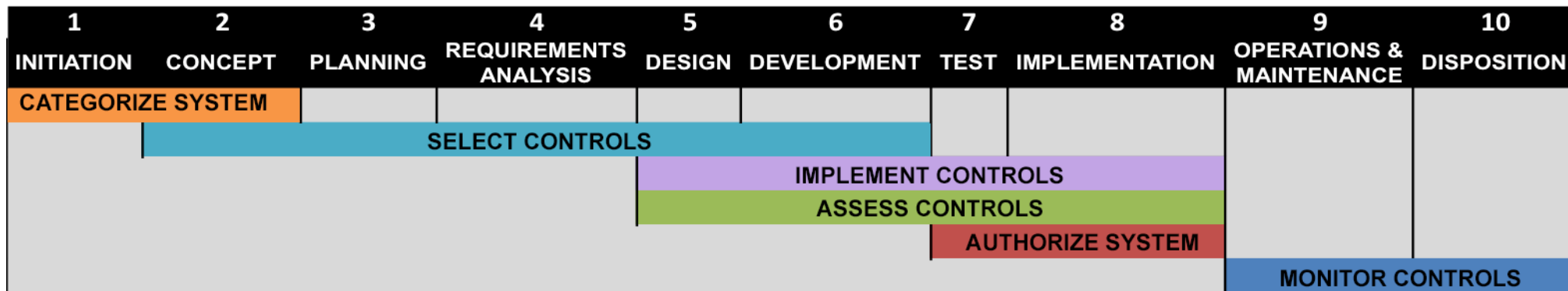
EPLC and the Risk Management Framework

CATEGORIZE THE SYSTEM AND SELECT CONTROLS

During this step:

The system is categorized; and

Controls are selected based on the system categorization.

Categorize the System
Risk Assessment

▸ **Risk assessment** or **risk analysis** is a process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

▸ The process incorporates threat and vulnerability analysis. It includes determining the likelihood that a security incident could occur, the resulting impact, and additional security controls that would mitigate this impact.

▸ Risk assessments should initially be conducted during the Initiation and Development stage of the EPLC. A risk assessment is also a required part of the security documentation for a security authorization.

Categorize the System
Determine Risk Impact Level

▸ FIPS 199 is used to determine the system categorization level of an IT system. Systems can be categorized as low, moderate, or high-impact for each of the security objectives: confidentiality, integrity, and availability.

▸ FIPS 200 is used to determine the system impact level, based on the categorization. Once the impact level is established, an appropriate set of controls, as identified in NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, can be chosen.

▸ NIST SP 800-60 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories is used to apply appropriate levels of controls for the system categorization.

Categorize the System
Risk Impact Assessment

FIPS 199 defines three categories of impact:

▸ **Low:** The potential impact is Low if the loss of confidentiality, integrity, and availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

▸ **Moderate:** The potential impact is Moderate if the loss of confidentiality, integrity, and availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

▸ **High:** The potential impact is High if the loss of confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Categorize the System
High Water Mark

▸ The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well.

▸ According to FIPS 200, a "high water mark" is the highest potential impact value assigned to each security objective for each type of information resident on those information systems.

Example 1
A system has two moderate risk applications and one high risk application residing on it, the overall impact rating is high.

Example 2
A system is categorized as low for availability, low for integrity, but high for confidentiality, the overall impact rating is high.

Select Controls

Control Selection

▸ Security controls are selected using NIST SP 800-53 Rev. 4 in combination with the low/moderate/high risk management guidance in FIPS 199 and FIPS 200.

▸ HHS security procedures and practices reflect the NIST and FIPS recommendations and requirements.

Select Controls

System Controls

NIST SP 800-53 Rev. 4 divides controls into families. There are 18 security control families and eight privacy control families. In previous revisions, controls were organized in three classes - Management, Operational, and Technical. Although class designations have been eliminated from Rev. 4, it may be useful for an organization to apply them to individual security controls and their components.

▸ **Management Controls:** Focus on the management of the computer security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management, through policy and documentation.

▸ **Operational Controls:** Address security issues related to mechanisms primarily implemented and executed by people (as opposed to systems). Often, they require technical or specialized expertise and rely upon management activities as well as technical controls.

▸ **Technical Controls:** Technical controls are security controls that are configured within the system. Technical controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Select Controls

Security Control Families

Management	Operational	Technical
• Security Assessments and Authorization • Planning • Risk Assessment • System and Services Acquisition • Program Management	• Awareness and Training • Configuration Management • Contingency Planning • Incident Response • Maintenance • Media Protection • Physical and Environmental Protection • Personnel Security • System and Information Integrity	• Access Control • Audit and Accountability • Identification and Authentication • System and Communications Protection

Categorize the System and Select Controls

Recap

▸ The categorization of the system directly effects the types of controls that are chosen for it.

▸ There are three categories of potential impact: low, moderate, or high.

- These three categories determine how secure a system must be to ensure confidentiality, integrity, and availability.

▸ NIST SP 800-53 Rev. 4 contains a catalog of 18 security control families and eight privacy control families.

IMPLEMENT AND ASSESS THE CONTROLS

During this step:

Most of the security documentation is produced; and

Controls are tested.

System Security Plan

▸ The System Security Plan (SSP) for each system includes necessary information for the Authorizing Official (AO) to grant an Authorization to Operate (ATO). The plan contains:

  – System identification, which includes the system owner, general description and purpose of the system, and equipment list;

  – A list of minimum security controls; and

  – Security documents that were developed during the EPLC.

▸ The SSP should be reviewed and updated or verified at least annually once the system is operational.

▸ If the system has changed (system environment, software, hardware, user groups, etc.), the SSP should be updated as soon as the change is made.

Contingency Plan

▸ A Contingency Plan for each system is required by law and includes the following key sections:

  – System criticality; Responsibilities; Business impact analysis; Preventive controls; Damage assessment; Recovery and reconstitution; and Backup requirements.

▸ IT Administrators may be involved in creating the Contingency Plan to ensure that it accurately captures what is possible in terms of technical recovery. IT Administrators also may be required to document changes as soon as they are made.

▸ Even when no changes have occurred, the document should be reviewed and verified by the IT Administrator at least annually.

Implement Controls

Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an assessment process for identifying and mitigating the privacy risks posed by an information system. It is required for every system. At a minimum, PIAs must analyze and describe the following:

▸ What information is to be collected;

▸ Why the information is being collected (e.g., to determine eligibility);

▸ Intended use of the information (e.g., to verify existing data); and

▸ With whom the information will be shared (e.g., another agency for a specified programmatic purpose).

Implement Controls

Privacy Impact Assessment

Additionally, PIAs must include information on:

▸ When and how individuals can consent to or decline particular uses of the information (other than required or authorized uses);

▸ How the information will be secured (i.e., management, operational, and technological controls); and

▸ Whether a system of records is being created under the Privacy Act of 1974.

Assess Controls

Security Control Assessment and Security Test & Evaluation

▸ A Security Control Assessment (SCA) is the formal evaluation of a system against a defined set of controls

▸ It is conducted in conjunction with or independently of a full Security Test and Evaluation (ST&E), which is performed as part of the security authorization.

▸ The SCA and ST&E will evaluate the implementation (or planned implementation) of controls as defined in the SSP. The results are the risk assessment report. This report will document the system's areas of risk.

▸ Types of system tests conducted include audits, security reviews, vulnerability scanning, and penetration testing.

Triggers for Updating Controls

▸ Security control assessments are conducted before the system is put into production and annually thereafter.

▸ In addition, common events should trigger administrators to recheck controls. For example:

  – NIST SP 800-53 is updated periodically based on comments from the IT security community to ensure the document reflects the most current controls used in practice. System administrators should verify they are using the most recent list of NIST controls and test the system against any new controls.

  – Routine changes in the immediate environment, such as:

    ▪ New or modified hardware;

    ▪ New or modified software (including applications and operating systems); and

    ▪ New threats introduced to the environment.

Assess Controls
Plan of Action and Milestones

▸ A Plan of Action and Milestones (POA&M) are a FISMA requirement to effectively manage security program risk and mitigate program-and system-level weaknesses.

▸ Effective POA&M management increases the awareness of an OpDiv's security posture, identifies systemic areas to address, and contributes to developing informed risk –based decisions.

▸ Every IT systems should have a POA&M to identify, manage, and mitigate weaknesses.

▸ All security and privacy weaknesses shall be recorded and managed in the POA&M. Sources of these weaknesses can come from many locations such as audit reports, a security authorization cycle, and incidents.

Assess Controls

Authorization Decision

▸ Authorization is required before a system may process, store, or transmit agency data. An AO or a designated representative reviews the security authorization package. The AO or designated representative will then give a system either an ATO or Denial of Authorization to Operate.

▸ An ATO signifies completion of an objective third party system evaluation and acceptance of any residual risk of the system to the agency. This means that the AO takes responsibility if a security incident related to a known risk were to occur.

▸ Denial of Authorization to Operate indicates that there are major weaknesses or deficiencies in the security controls employed within or inherited by the information system. This rarely occurs if the processes outlined in the EPLC Framework Overview are followed.

Implement and Assess Controls

Recap

▸ Most of the security documentation is finalized during this step.

▸ The documentation is used by the AO to determine if an ATO should be issued for the system.

▸ Every system must have an SSP, Risk Assessment, and ATO to operate. A POA&M is also required when weaknesses are identified.

EPLC and the Risk Management Framework

MONITOR THE CONTROLS & SYSTEM DISPOSAL

During this step:

Controls are monitored and periodically tested; and

Plans are made to securely terminate the system.

Monitor Controls

Configuration Management

▸ Once operational, systems are typically in a constant state of modification and enhancement, such as upgrades to components.

▸ Any change can have a significant impact on the security posture of the system. Therefore, continually documenting system changes and assessing the potential impact on the security is an essential aspect of maintaining system accreditation.

▸ Adherence to your OpDiv's configuration and change management procedures is necessary to maintain an accurate inventory of all changes to the system.

Monitor Controls
Patch Management

▸ Part of maintaining a system is to ensure system components are kept up-to-date with patches. Effective patch management entails **maintaining an awareness of system vulnerabilities and available patches** for mitigation. Patches are periodically released for operating systems, office suites, commercial software tools and applications, and commonly used utilities.

▸ Patches should be **tested before deployment** to a production environment to prevent adverse impacts to operational systems.

Monitor Controls

Continuous Monitoring

▸ FISMA requires periodic and continuous testing and evaluation of the security controls to ensure that they remain effective.

▸ The ongoing monitoring of security controls can be accomplished by one or a combination of the following:

- Security review;

- Security testing;

- Evaluation or audit; and

- Software/Hardware tools.

System Disposal

Disposal of System Components

Media sanitization is important either at the end of the system's life cycle or at any point when new hardware or media is replacing existing hardware or media.

System disposal has five parts as stated in NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*:

▸ **Building and Executing a Disposal/Transition Plan** ensures that all stakeholders are aware of the future plan for the system and its information. This plan should account for the disposal / transition status for all critical components, services, and information.

▸ **Information Preservation** ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.

Disposal of System Components (Continued)

▸ **Media Sanitization** ensures that data is deleted, erased, and written over as necessary to retain confidentiality.

▸ **Hardware and Software Disposal** ensures that hardware and software is disposed of as directed by the Information Systems Security Officer (ISSO).

▸ **System Closure** ensures that the information system is formally shut down and disassembled.

For additional information, see the *HHS-OCIO Policy for Information Systems Security and Privacy* and *NIST SP 800-88, Guidelines for Media Sanitization*.

System Disposal

Planning for Disposal

▸ Disposing of systems is a predictable occurrence. Planning ahead for the integration of security measures into the replacement process helps you securely and conscientiously manage both disposal and introduction of new hardware or software.

▸ Ensure that the purchase and installation of new equipment does not conflict with the proper disposal of data and old equipment. This prevents creating unnecessary vulnerabilities or an incident which could cause embarrassment to or damage the reputation of HHS.

▸ **Always take time to dispose of systems hardware and media properly!**

Monitor Controls & System Disposal

Recap

▸ Once a system is operational, controls should be monitored for effectiveness and tested periodically.

▸ Changes in the configuration of the system could significantly impact security.

▸ It is critical to properly dispose of information systems and archive the data they contain. Plan and budget for disposal of the system early.

EPLC and the Risk Management Framework

Recap

▸ The six steps of the RMF are integrated across the ten phases of the EPLC to improve security and strengthen risk management processes.

▸ Each phase requires activities and deliverables to ensure that security is addressed throughout the life of the IT system.

Incident Handling

Incident Handling

Incident Handling Lifecycle Overview

▸ Per NIST SP 800-61 Rev. 2, *Computer Security Incident Handling Guide*, incident management entails**:**

- – Preparation;
  - ▪ Ensuring the proper policies and procedures, lines of communication and team members are identified prior to an incident occurring.

- – Detection & Analysis; *("Identification" at HHS)*
  - ▪ Identifying and differentiating an incident from an event. This includes gathering, and initial triaging of all available data associated with the incident.

- – Containment, Eradication, and Recovery; and
  - ▪ Initiated to seclude affected hosts and systems from the network, initiating network blocks on adversaries, etc; address issues then bring the network/system back to production status.

- – Post-Incident Activity *("Lessons Learned" at HHS)*
  - ▪ Notes and lessons learned from the response are evaluated, and in turn, used to improve the security landscape by improving patching methodologies, reevaluating access permissions, account usage, user training, etc.

Incident Handling
Preparation

▸ Each OpDiv has an incident handling plan, consisting of:

– Policies and procedures;

– System documentation;

– Incident Response Team (IRT); and

– Monitoring, communication, and mitigation tools.

Incident Handling

Detecting and Analyzing Incidents

▸ Detecting potential security incidents may be difficult. Knowing how a system usually behaves and learning which symptoms can indicate potential incidents is a way to recognize when to further investigate.

▸ Correlation and analysis of events may help to identify potential incidents that may have been overlooked and could become a more serious problem. Early awareness of potential incidents can stop damage, disclosure, and other harmful effects before they happen.

▸ Incident detection and analysis may take several individuals reviewing activity before it is realized that an incident has occurred.

▸ Within HHS, users should report all suspected computer security incidents to their OpDiv Computer Security Incident Response Team (CSIRT) or Help Desk.

▸ For more information on incident reporting, please visit: http://www.hhs.gov/ocio/securityprivacy/incidentmanagement/incidentresp.html.

Incident Containment

▸ There is a delicate balance between protecting evidence from an incident and containing an incident to prevent further impact. If evidence is destroyed, it may be difficult to determine the root cause and prosecute the attacker.

▸ Containment strategies vary based on the type of incident. Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources;

- Need for evidence preservation;

- Service availability (e.g., network connectivity, services provided to external parties);

- Time and resources needed to implement the strategy;

- Effectiveness of the strategy (e.g., partially contains the incident, fully contains the incident); and

- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Incident Handling

Incident Eradication and Recovery

▸ After an incident has been contained and evidence preserved, as appropriate, **eradication** may be necessary to eliminate components of the incident. Deleting malicious code and disabling breached user accounts are examples of eradication. For some incidents, eradication is either not necessary or is performed during recovery.

▸ During **recovery**, IT Administrators restore systems to normal operation and, as necessary, harden systems to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and adding or strengthening other security controls.

Post-Incident Activity

▸ As an IT Administrator, you may be asked to participate in "lessons learned" exercises with the OpDiv IRT to discuss:

- Exactly what happened, and at what times?

- How well did staff and management perform in dealing with the incident?

- Were the documented procedures followed?

- Were they adequate?

- What information was needed sooner?

- Were any steps or actions taken that might have inhibited the recovery?

- What would the staff and management do differently the next time a similar incident occurs?

- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Incident Handling: Your Role

▸ Incident handling plans are documented for systems to ensure computer security incidents are handled efficiently and effectively.

▸ Each OpDiv is responsible for developing and documenting the process and responsibilities for incident handling.

▸ IT Administrators are most likely to be involved in the Detection, Response, and Resolution phases of the incident handling life cycle.

> Federal agencies are required by law to report incidents involving Personally Identifiable Information (PII) to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery.

Incident Handling

Incident Handling: Your Role – Reporting

▸ HHS defines an **incident** as the violation, or an imminent threat of a violation, of an explicit or implied security policy, acceptable use policies, or standard security practices in a computing or telecommunications system or network.

▸ Immediate and effective reporting may help prepare for future incidents, and prevent incidents from recurring. Incident reporting shares knowledge across HHS OpDivs and can reduce the likelihood of future occurrences.

▸ Be sure to follow incident reporting procedures while an incident is being handled and document each step toward resolution.

Incident Handling
Privacy Incident Response Team

▸ A privacy incident requires coordination, collaboration, and communication between the Department and the affected OpDiv.

▸ The Privacy Incident Response Team (PIRT) oversees the response efforts and activities for suspected or confirmed privacy incidents for the Department.

▸ The PIRT must review any communication, such as a notification letter, before an OpDiv contacts a potentially impacted individual and will review OpDiv recommendations to provide credit monitoring to an individual at risk for identity theft.

Incident Handling
Recap

▸ Each OpDiv has an incident response plan which describes how to respond when an incident occurs.

▸ Federal agencies are required by law to report incidents involving PII to the US-CERT within one hour of discovery.

▸ IT Administrators may be asked to help in any of the four areas of incident management:

- Preparation;

- Detection & Analysis;

- Containment, Eradication, and Recovery; and

- Post-Incident Activity.
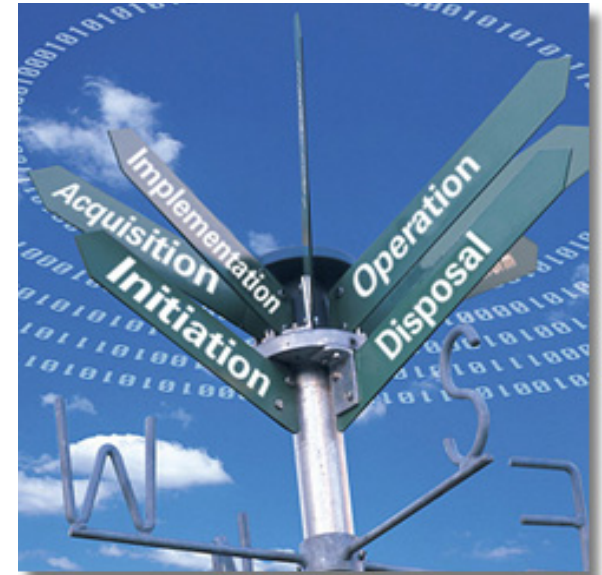
User Access
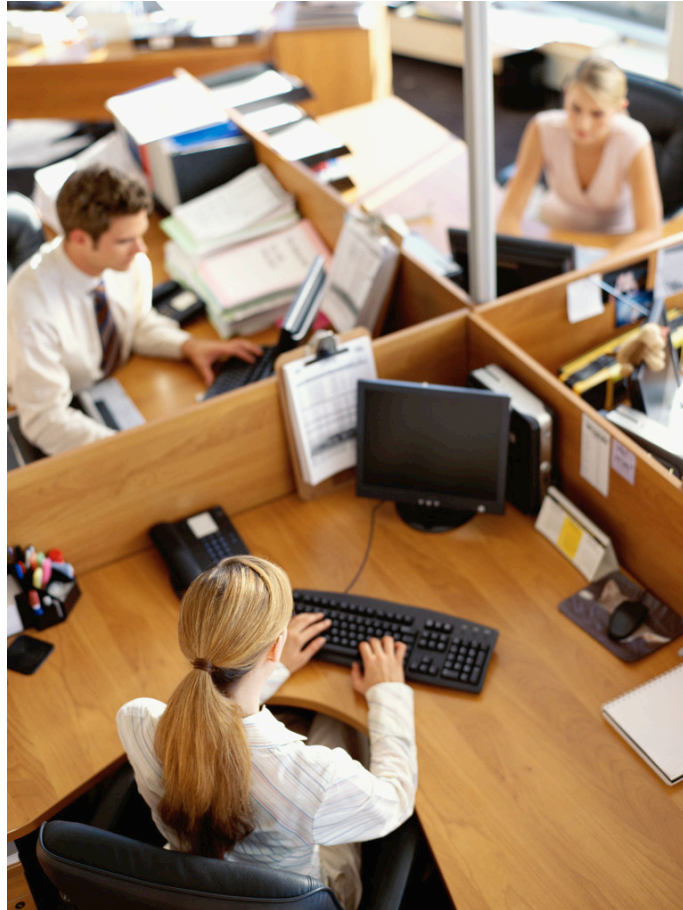
User Access

Introduction

Your job as an IT Administrator gives you a great deal of technical influence over the system. To comply with Federal policies and regulations, and good practices, it is important to observe separation of duties guidelines.

User Access

Level of Access

▸ **Access controls** exist to ensure that only authorized individuals gain access to information system resources, that they are assigned an appropriate level of privilege, and that they are individually accountable for their actions.

▸ At HHS, system access administrators or designees process all internal requests for access. Access is granted according to the most restrictive set of rights or privileges needed. The data owner is responsible for specifying the type of user access which may be approved.

Rules of Behavior and User Access

▸ **The Rules of Behavior For Use of HHS Information Technology Resources (HHS Rules of Behavior)** describe the user responsibilities and expected behavior with regard to information system usage. **All users accessing Department systems and networks are required to read and sign the HHS Rules of Behavior indicating that they understand and agree to abide by the rules** *before* **receiving access**[1].

▸ IT Administrators monitor system access to ensure that there is not an excessive or unusual number of individuals receiving high level or administrator–level access to the system. This could indicate a lack of controls–including least privilege and "need to know" controls.

▸ In general, individuals that are administering the system should not be responsible for auditing or reviewing the system or its controls.

[1]Some OpDivs have their own Rules of Behavior which users must read and sign before accessing the network or data.

User Access

Monitoring User Access/Recertification

▶ Periodic recertification of user access ensures system access is limited to those who have a current business purpose.

▶ System user account status is reviewed by IT Administrators on a defined recurrence and reported to the ISSO and to supervisors/managers.

▶ Inactive accounts are terminated within an OpDiv-defined timeframe unless the user's supervisor provides written certification of the need for continuation of access. Accounts for separated employees, contractors, volunteers, or others no longer requiring access are terminated immediately.

User Access

Terminating User Access

▸ It is important to terminate user access promptly when an individual has separated from HHS. Separations can be due to termination of employment, retirement, or transfer. Terminations can potentially be hostile situations.

▸ In general at HHS, for routine separations, termination of user access occurs within 24 hours of the separation. For potentially hostile terminations, access is terminated at the exact time of employee notification.

▸ **Take time to discuss termination of access procedures with your supervisor if you do not know how this is handled for your system.**

User Access

Recap

▸ Monitoring user access and monitoring privileged users is critical to the security of information systems.

▸ User access should be limited to a need to know basis. It should be periodically reviewed, and removed if access is no longer required.

▸ The HHS Rules of Behavior must be signed before a user can access the network or the systems on the network.

Summary

Summary

Conclusion

At one time, IT Administrators were only responsible for traditional administrative tasks for systems they supported. The role of securing systems belonged to someone else. However, due to the ever-changing risk environment brought about by the interconnection of systems, all parties involved with systems have a role in securing them.

Summary

Objectives

You are now able to:

✓ Understand your role and responsibilities to protect information security as an IT Administrator.

✓ Define the basic components of an information security program.

✓ Identify governing bodies and legislative drivers for protecting information security.

✓ Understand the EPLC and RMF and how they relate to the development of IT systems.

✓ Understand the basics of responding to a security or privacy incident.

✓ Understand the basics of access control.

✓ Identify where to locate HHS policies, procedures, and guidance for developing, implementing and managing information systems from beginning to end.

Appendix

HHS Resources

▸ The **HHS Cybersecurity Program** is the Department's enterprise-wide information security and privacy program, helping to protect HHS against potential IT threats and vulnerabilities. The Program plays an important role in protecting HHS' ability to provide mission-critical operations, and is an enabler for e-government.

▸ HHS Cybersecurity Program Support provides assistance with IT security and privacy related issues. HHS Cybersecurity Program Support is staffed Monday through Friday from 8:00 AM to 5:00 PM eastern standard time (EST).

Web: HHS Cybersecurity Program

Phone: (202) 205-9581

E-mail: HHS.Cybersecurity@hhs.gov

Appendix

HHS Resources

▸ The *HHS-OCIO Policy for Information Systems Security and Privacy* is available at: http://www.hhs.gov/ocio/policy/index.html.

▸ The *Enterprise Performance Life Cycle Frame*work *Overview Document* provides detailed information about how to complete each phase of the EPLC. It can be found at: http://www.hhs.gov/ocio/eplc/index.html.

▸ Templates, practice guides, checklists and other artifacts used throughout the EPLC process, including the Stage Gate Reviews template can be found at: http://www.hhs.gov/ocio/eplc/Enterprise%20Performance%20Lifecycle%20Stage%20Gate%20Reviews/eplc_stage_gate_reviews.html.

Appendix

Legislation and Guidance

▸ **Legal Requirements**

- Public Law 107-347, *E-Government Act of 2002*, Title III, Federal Information Security Management Act, December 2002.

- Office of Management and Budget Circular A-130, *Appendix III, Security of Federal Automated Information Resources*, November 2000.

- Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004.

- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 1998.

- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.

▸ **Standards**

- NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

- NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006.

Appendix

Legislation and Guidance

‣ **NIST Guidance**

- NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

- NIST SP 800-27 Rev. A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

- NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* February 2010.

- NIST SP 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

- NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations, May 2013.*

- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.

Appendix

Legislation and Guidance

- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

- NIST SP 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

- NIST SP 800-61 Rev. 1, *Computer Security Incident Handling Guide*, March 2008.

- NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle,* October 2008.

- NIST SP 800-70 Rev. 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.

- NIST SP 800-88, *Guidelines for Media Sanitization,* September 2006.

HHS Rules of Behavior for Privileged User Accounts and Acknowledgement

On the next few slides, you will read and acknowledge the HHS Rules of Behavior for Privileged User Accounts.
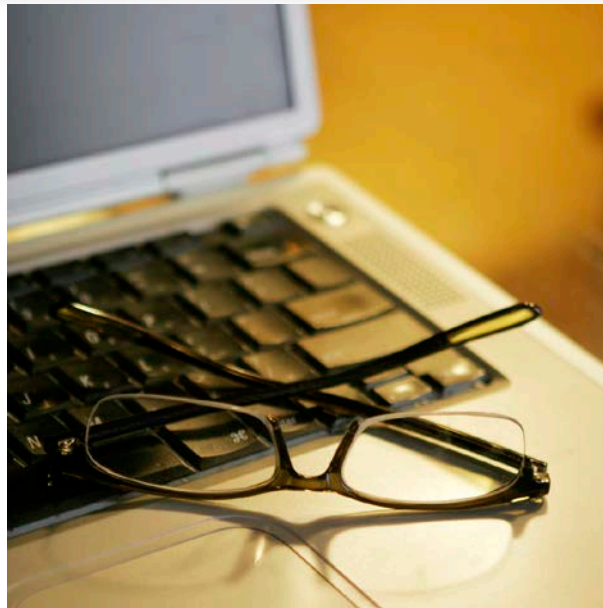
HHS Rules of Behavior for Privileged User Accounts

Addendum: HHS Rules of Behavior for Privileged User Accounts

The *HHS Rules of Behavior for Privileged User Accounts* is an addendum to the *HHS Rules of Behavior for Use of Information Resources* (HHS RoB) and provides common rules on the appropriate use of all HHS information technology resources for all Department Privileged Users,[1] including federal employees, interns, and contractors. Privileged User account roles have elevated privileges above those in place for general user accounts regardless of account scope (e.g., both local and domain administrator accounts). Potential compromise of Privileged User accounts carries a risk of substantial damage and therefore Privileged User accounts require additional safeguards.

All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgement form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role. The same signature acknowledgement process followed for the HHS RoB applies to the Privileged User accounts. Each Operating Division (OpDiv) must maintain a list of Privileged User accounts.

I understand that as a Privileged User, I must:

- Protect all Privileged User account passwords/passcodes/Personal Identity Verification (PIV) personal identified numbers (PINs) on Low, Moderate, and High systems;
- Comply with all system/network administrator responsibilities in accordance with HHS policy;
- Use my Privileged User account(s) for official administrative actions only;
- Notify system owners immediately when privileged access is no longer required; and
- Complete any specialized role-based security or privacy training as required before receiving privileged system access.

[1]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..

HHS Rules of Behavior for Privileged User Accounts

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

- Share Privileged User account(s) or password(s)/passcode(s)/PIV PINs;
- Install, modify, or remove any system hardware or software without system owner written approval;
- Remove or destroy system audit, security, event, or any other log data;
- Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls;
- Introduce unauthorized code, Trojan horse programs, malicious code, or viruses into HHS information systems or networks;
- Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses;
- Use Privileged User account(s) for day-to-day communications;
- Elevate the privileges of any user without prior approval from the system owner;
- Use privileged access to circumvent HHS policies or security controls;
- Use a Privileged User account for Web access except in support of administrative related activities; or
- Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.

HHS Rules of Behavior for Privileged User Accounts Acknowledgement

ACKNOWLEDGEMENT PAGE

I have read the *HHS Rules of Behavior for Privileged User Accounts* (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the *HHS Rules of Behavior for Privileged User Accounts* or information security policies and standards may lead to 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 the *HHS Rules of Behavior for Privileged User Accounts* must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the *HHS Rules of Behavior for Privileged User Accounts* draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

APPROVED BY AND EFFECTIVE ON:
_____/s/_____ ____ __July 24, 2013_____

The record copy is maintained in accordance with GRS 1, 18.a.

Congratulations

You have completed the **Information Security for IT Administrators** course.