Office of Information Resource Management
Office of the Assistant Secretary for Management and Budget
Department of Health and Human Services

HHS IRM Policy for IT Security for Remote Access

January 8, 2001

Project:	HHS IRM Policy
Document Number:	HHS-IRM-2000-0005

Table of Contents

1. Purpose

This document establishes the policies and procedures that are to be followed to assure that the Department=s information technology (IT) resources are appropriately protected when authorizing the remote access of HHS automated information and systems.

2. Background

It is the Department of Health and Human Services= (HHS=) intent to implement an Information Technology (IT) Security Program that complies with federal laws, regulations, and directives and communicates uniform policies for the protection and control of Information Technology (IT) resources directly or indirectly relating to the activities of the Department.

It is HHS= policy as documented in the "HHS Automated Information Systems Security Handbook" to implement an automated information systems (AIS) security program to assure that its automated information and systems have a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information or system.

Telework arrangements requiring remote access to IT resources are powerful tools if implemented correctly, e.g.:

- Employees, whose work meets management's criteria for working off-site, have greater flexibility and higher morale;
- Managers can effectively manage off-site employees; and
- For the public, there is potential for reduced traffic congestion and environment pollution.

While offering potential benefits, remote access to IT resources introduces new risks to the security of HHS= automated information and systems, as well as to the privacy of the clients HHS serves. For example, without appropriate safeguards to protect the integrity of the electronic functions and processes the employee working remotely is to perform, the following security issues could occur:

- Confidential information could be unintentionally disclosed;
- Sensitive data could be altered or deleted;
- Malicious software could be introduced to the user and/or HHS office equipment; and
- Systems sign-on identifications and passwords could be intercepted and reused to access systems and data files without authorization.

Thus, taking the time to identify, implement, and use appropriate safeguards is required if HHS is to protect the integrity of the electronic processes when accessing IT resources remotely. In addition, similar security concerns exist for users who use remote access techniques to access HHS systems and information from their normal work sites. IT security practices must be viewed as enablers without which telework, and other remote access work arrangements could

not be allowed. Enhanced telecommunications resources allow employees to work at home or other virtual office environments (e.g., from special telecommuting centers or while on travel), have access to HHS data for authorized use, and maintain contact with co-workers and managers while away from their official HHS work site. Given the ubiquitous nature of the IT client landscape, an appropriate architecture for secure remote access is dependent on tiered authentication based on risk and vulnerability and a viable, well managed intranet solution.

3. Scope

The policy contained in this document is applicable to all HHS IT resources, at all levels of sensitivity, whether maintained by HHS or by a contractor on behalf of HHS. This policy is mandatory for all organizational units, Operating Divisions (OPDIVs), employees, and contractors when using HHS IT resources who process, store, transmit, or have access to HHS IT resources. This policy applies to all existing automated systems and to any new systems technology acquired after the effective date of this policy.

This policy does not apply to telework arrangements when telework does not involve remote access.

4. Policy

When authorizing the remote access of HHS automated information and systems the following applies: (Note: This policy only applies to telework programs when the employee will be required to use a computer to remotely access HHS IT resources.)

4.1. DEPARTMENTAL ORGANIZATIONS

Operating Divisions and other departmental organizations shall adopt policies and procedures that:

4.1.1. Assess the sensitivity and criticality of information and systems to be used or accessed at the remote site and establish appropriate security protections (i.e., the security safeguards and procedures should be cost/beneficial compared to the risk and commensurate with the need to protect the integrity of the processes the employee or contractor is expected to perform).

4.1.2. When accessing sensitive HHS= IT resources (except for publicly available web sites), assure that all electronic communications over the Internet between authorized users and HHS are encrypted. (Refer to applicable standards identified in HHS= Information Technology Architecture [ITA].)

4.1.3. Provide authentication through, for example, the use of passwords, personal identification numbers (PINs), user identification names, biotechnology (e.g., retina or fingerprint scans), or the use of digital signature or smart tokens technology. (Refer to applicable standards identified in HHS= Information Technology Architecture.)

4.1.4. Provide periodic employee training in the use of all equipment, software, and security safeguards.

4.1.5. Assure that users are aware that the unauthorized or improper use of Government office equipment could result in loss of use or limitations on use of equipment, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of damages resulting from any unauthorized use.

4.1.6. Develop a management/employee agreement that, at a minimum, outlines the work that the participating employee is authorized to perform, management work expectations, and the data to be used in performing expected duties, as well as the security safeguards and procedures the employee is expected to follow.

4.1.7. The organization shall ensure appropriate encryption, authenticity non-repudiation, secure storage of files, removal and non-recovery of temporary files created in processing sensitive data, virus protection and intrusion detection at the

level required by the Department. If the organization is unable to comply then the organization shall provide all workstation or other necessary equipment (e.g., laptops or personal computers [PC's]) and software configured to the OPDIV standard along with needs for assembly, servicing, and maintenance.

4.1.8. Establish mechanisms to backup data created and/or stored at the alternate work site. For example, an employee should store files on a shared file server located at the HHS designated site since servers shall be backed up daily.

4.1.9. Assure that e-mail access from any source shall be secure and encrypted (e.g., secure socket layer sessions).

4.2. EMPLOYEES

Employees shall:

4.2.1. Report any security incident (or suspected incident) to management as soon as possible during or after it occurs according to the HHS IRM Policy for Establishing an Incident Response Capability, HHS-IRM-2000-0006.

4.2.2. Use HHS provided equipment and software for authorized activities only. Employees are prohibited from using such equipment for private or inappropriate purposes (Refer to IRM Policy for Personal Use of HHS Information Technology Resources, HHS-IRM-2000-003).

4.2.3. Protect HHS equipment and data from intentional or accidental alteration (including data deletion), theft, or breach of confidentiality by any or all of the following, as appropriate:

- Storing all sensitive data in encrypted form;
- Using and securely storing removable storage media;
- Using physical or cyber locks;
- Place workstations in secure areas;
- Refrain from sharing passwords or other secure information with other individuals.

4.2.4 Agree to permit periodic inspections of Government-owned IT equipment and software the employee is using to ensure proper maintenance (e.g., to install software updates and security patches) and provide the employee with at least two business days advance notice.

4.2.5 Agree to allow HHS to install and apply new or enhanced software and hardware. HHS shall provide at least two business days advanced notice unless the update is deemed a security emergency.

4.2.6 Apply required safeguards (refer to Section 4.1.1) to protect Government/agency records from unauthorized disclosure or damage and comply with the Privacy Act requirements set forth in the Privacy Act of 1974, Public Law 93-579, codified at Section 552a, Title 5 U.S.C.

5. Roles and Responsibilities

Information systems security responsibilities and accountability shall be explicit. The responsibilities and accountability of owners, providers, and users of computer systems and data and other parties concerned with the security of information systems shall be documented.

5.1. The HHS Chief Information Officer (CIO)

The HHS CIO is responsible for establishing and implementing the information security policies to assure that HHS systems and data are secure and protected from unauthorized access. This responsibility is delegated to the Deputy Assistant Security for Information Resources Management.

5.2. The HHS Senior Information System Security Officer

The HHS Senior Information System Security Officer is responsible for developing and disseminating information concerning recommended safeguards, and the potential security threats and concerns of remote access of HHS automated information and systems.

5.3. The OPDIV CIOs

OPDIV CIOs are responsible for:

5.3.1. Implementing the policy, procedures, and practices to assure that OPDIV systems, programs, and data are secure and protected from unauthorized access that might lead to the alteration, damage, destruction, or theft of automated resources, unintended release of data, and denial of service; and

5.3.2. Ensuring that all OPDIV employees and contractors comply with this policy.

5.4. The OPDIV Information System Security Officers

The OPDIV Information System Security Officers are responsible for the following:

5.4.1. Ensuring that all OPDIV personnel are aware of this policy and incorporating it into telework and remote access briefings and training programs; and

5.4.2. Promptly notifying the Departmental IT Security Officer of computer security incidents (or suspected incidents) resulting from remote access.

5.4.3. Assuring that information security notices and advisories are distributed to appropriate OPDIV personnel and that vendor issued security patches are installed on HHS software expeditiously.

5.5. Supervisors and Managers

Supervisors and managers shall ensure that:

5.5.1. An appropriate Management/Employee Agreement is signed by every employee approved for telework; and

5.5.2. Their staffs (Federal and contractor resources) have been trained concerning their security responsibilities, including the need to report any computer security incidents (or suspected incidents), when remotely accessing HHS information and systems or when teleworking.

5.6. Employees

Employees must sign and agree to abide by the provisions, requirements, and expectations of the Management/Employee Agreement.

6. Applicable Laws/Guidance

The following public laws and Federal regulations and guidance are applicable to this policy circular:

- Computer Fraud and Abuse Act of 1986 (P.L. 99-474)
- Computer Security Act of 1987 (P.L. 100-235)
- Privacy Act of 1974 (P.L. 93-579)
- Clinger-Cohen Act (Information Technology Management Reform Act of 1996 - Division E of P.L. 104-106)
- Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Resources, Appendix III, Security of Federal Automated Information Resources
- Presidential Decision Directive 63 (PDD-63), Critical Infrastructure Protection, May 22, 1998
- July 11, 1994, President Clinton memorandum adopting the National Performance Review Program recommendation for expanded opportunities for Federal workers to participate in a flexible work arrangement.
- June 21, 1996, President Clinton memorandum to Executive Heads of Departments and Agencies, Implementing Federal Family Friendly Work Arrangements
- HHS Information Technology Architecture developed by HHS Information Technology Architecture Group, Assistant Secretary for Management and Budget, Deputy Assistant Secretary for Information Resources Management (April 2000)
- HHS' Automated Information Systems Security Program Handbook
- 5 CFR 2635 ▭ Standards of Ethical Conduct for Employees of the Executive Branch
- Part 1 of Executive Order 12674 ▭ Implementing Standards of Ethical Conduct for Employees of the Executive Branch
- 41 CFR 101-35. 201 - Telecommunications Management Policy

7. Information and Assistance

Direct questions, comments, suggestions or requests for further information to the Deputy Assistant Secretary for Information Resources Management, (202) 690-6162.

8. Effective Date/ Implementation

The effective date of this policy is the date the policy is approved.

OPDIVs shall have two years from the ^Effective Date▭ to fully comply with this policy.

These policies and procedures will not be implemented in any recognized bargaining unit until the union has been provided notice of the proposed changes and given an opportunity to fully exercise its representational rights.

The HHS policies contained in this issuance shall be exercised in accordance with Public Law 93-638, the Indian Self-Determination and Education Assistance Act, as amended, and the Secretary's policy statement dated August 7, 1997, as amended, titled "Department Policy on Consultation with American Indian/Alaska Native Tribes and Indian Organizations." It is HHS' policy to consult with Indian people to the greatest practicable extent and to the extent permitted by law before taking actions that affect these governments and people; to assess the impact of the Department's plans, projects, programs, and activities on tribal and other available resources; and to remove any procedural impediments to working directly with tribal governments or Indian people

9. Approved

/s/ 01/08/01
John J. Callahan DATE
Assistant Secretary for Management and Budget

Glossary

Authorized Telework - Authorized telework is work performed by an employee away from his or her duty station that requires connectivity for data transmission.

Information Technology (IT) – IT is equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Remote Access – Remote Access is computer access to HHS networks or systems by authorized users accessing HHS automated information and systems from outside the protection of agency firewalls.

Remote Access Connections – Remote access connections are resource components required to provide remote access to the HHS networks (e.g., hardware, software, service, link/signal). Requirements will vary depending on the remote access location and work to be performed.

Security Incident – A security incident is an event that may result in, or has resulted in the unauthorized access to, or disclosure of, sensitive or classified information; unauthorized modification or destruction of systems data; reduced, interrupted, or terminated processing capability; malicious logic or virus activity; or the loss, theft, damage, or destruction of any IT resource.

Telework - Telework describes a specific computing environment that uses automated information resources over a distance to accomplish work activities. As defined by the National Institute of Standards and Technology (NIST), telecommuting (or telework) is the use of telecommunications to create an ^office@ away from the established (physical) office. The telecommuting office may be an employee=s home, a hotel room or conference center, an employee=s travel site, or a telecommuting center. The telecommuter=s office may or may not have the full computing functionality of the established office depending on the needs of the individual employee.

Telecommuting Centers - Telecommuting Centers are office units generally located in the outlying edge of the commuting area and often shared by multiple organizations. Each Center is equipped with workstations and services to enable an employee to accomplish his or her official duties without commuting to the main duty station.