

Appendix R
Certification and Accreditation Statements
For The
Defense Occupational and Environmental Health Readiness System
Data Repository, Version 1.5.1
(DOEHRS-DR 1.5.1)

15 September 2004

	<p>MHS Advanced Technology Innovation Center Three Skyline Place - 5201 Leesburg Pike, Suite 1600 Falls Church, VA 22041</p>	 Health Affairs
---	---	--

For Official Use Only



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, DC 20301-1200

**Certification Statement
for
Defense Occupational and Environmental Health Readiness System – Data Repository,
Version 1.5.1 (DOEHRS-DR 1.5.1)
Approval To Operate (ATO)**

Based on the results of the security evaluation dated 15 September 2004, I have determined that, with closure of the identified short-term risks, adequate security measures will have been taken to grant an Approval to Operate (ATO) to the currently accredited DOEHR-DR 1.5.1.

I have reviewed the findings and recommendations of the JMISO Certification Team, and conclude that DOEHR-DR 1.5.1 will have satisfied the baseline security requirements of the Department of Defense (DoD) and the Military Health Service (MHS). Identified vulnerabilities have been mitigated by DOEHR-DR 1.5.1 and validation of mitigation by the Certification Team was completed on 16 August 2004. There are eleven (11) remaining vulnerabilities identified as short-term risks and residual risks, and these risks are rated as One (1) Medium and ten (10) low. I recommend that the DAA approve the DOEHR-DR 1.5.1 and grant an Approval to Operate for a period of three (3) years from the date of signature of the DOEHR-DR 1.5.1 Accreditation Statement with the following additional terms and conditions:

1. General Conditions:

- a. If the Resources Information Technology Program Office (RITPO) makes any changes to the configuration of DOEHR-DR 1.5.1, the Program Office (PO) must assess and document the impact on the security policies and processes. This involves fully understanding any changes that are made to the security policies and processes, documenting any new vulnerability, conducting elimination or mitigation to reduce risk, and finally updating SSAA and supporting documents. The JMISO Certification Team must be notified, and provided a copy of the updated security documents.
- b. The PO must use the following guidelines in determining the level of certification activities required when changes are made to the configuration of DOEHR-DR 1.5.1:
 - 1) If the PO deems the changes to the configuration to be “minor”, the changes can be documented using Release Notes that have a security section. An example of a “minor” change would be the addition of functional changes that do not make any changes to the security policies and procedures.

For Official Use Only

- 2) If the PO deems the changes to the configuration to be more than “minor” but still less than a “major” change, a Risk Assessment must be coordinated with and validated by the JMISO Certification Team. The results normally will be documented as an addendum to the system accreditation report. An example of this type of change would be the addition of a new Commercial-Off-The-Shelf (COTS) product to the application or, adding one or more new interfaces to the system.
 - 3) If the PO deems the changes to the configuration to be a “major” change, a full Certification and Accreditation effort that leads to an Approval to Operate (ATO) must be performed by the JMISO Certification Team. Examples of “major” changes include changing the operating system, or changing a major component, such as the database used by the system.
- c. Mitigation of any of the system’s technical risks, identified under “Specific Conditions”, below, is not to be delayed for the duration of the approved certification, but rather completed by the PO as quickly as resources permit.

2. Specific Conditions:

- Take all appropriate actions to close the Medium risk indicated in this report, or reduce this risk to a Low rating and to the extent that it may be considered an acceptable residual risk to the operation of DOEHRS-DR 1.5.1. The JMISO Certification Team and the PO will coordinate efforts, prior to 01 December 2004, to allow JMISO verification that this task is completed
- Establish and document a procedure to ensure that the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA), including Appendices, is reviewed and updated as necessary upon any significant change to the system security or configuration and, at least, on an annual basis. DOEHRS-DR 1.5.1 will validate this action to the JMISO Certification Team prior to 01 December 2004
- Initiate efforts to establish an alternate site for DOEHRS-DR 1.5.1 at a location physically separate from APG in Aberdeen, Maryland

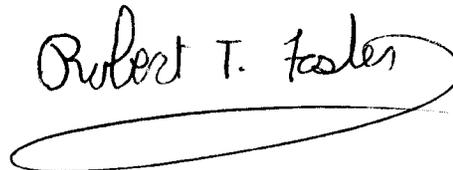
3. Other:

Best practices and JMISO policy will require DOEHRS-DR 1.5.1 to resolve any relevant issues relating to the upcoming discontinuation of Microsoft support of Windows NT. Although not considered a risk for the purposes of this Certification and Accreditation, these circumstances create a business risk because systems will be removed from Service networks if Windows NT is running and unsupported.

Further, I recommend that the DAA require all of the above conditions to be satisfied as soon as possible and no later than the next Annual Review for DOEHRS-DR 1.5.1, unless a specific date is designated within a condition.

For Official Use Only

These conditions are attached to Appendix R of the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA).

A handwritten signature in black ink that reads "Robert T. Foster". The signature is enclosed within a large, hand-drawn oval.

Robert T Foster, CHE
Certifying Authority
Military Health System
Joint Medical Information System Office (JMISO)

Date: 15 Sept 2004

For Official Use Only



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

**Accreditation Statement
for
Defense Occupational and Environmental Health Readiness System – Data
Repository
(DOEHRS-DR 1.5.1)
Approval To Operate (ATO)**

Having examined the evaluation report dated 15 September 2004, its findings and recommendations, and weighing operational requirements and current system risk exposures, it is declared that it is appropriate to grant DOEHRS-DR 1.5.1 an Approval to Operate (ATO) and to issue this Accreditation Statement effective for three (3) years from the date of signature below.

The granting of this Approval to Operate is contingent on DOEHRS-DR 1.5.1 compliance with conditions specified in Appendix R of the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA).

A handwritten signature in black ink, appearing to read "M.A. Lyford".

Mark A. Lyford
COL, MS, USA
Designated Approving Authority
Joint Medical Information System Office
(JMISO)

Date: 15 Sep 04

For Official Use Only

ATTACHMENT A
TERMS AND CONDITIONS
of the
APPROVAL TO OPERATE (ATO)
for
Defense Occupational and Environmental Health Readiness System – Data
Repository
(DOEHRS-DR 1.5.1)

For Official Use Only

1. General Conditions:

- a. If the Resources Information Technology Program Office (RITPO) makes any changes to the configuration of DOEHRS-DR 1.5.1, the Program Office (PO) must assess and document the impact on the security policies and processes. This involves fully understanding any changes that are made to the security policies and processes, documenting any new vulnerability, conducting elimination or mitigation to reduce risk, and finally updating SSAA and supporting documents. The JMISO Certification Team must be notified, and provided a copy of the updated security documents.
- b. The PO must use the following guidelines in determining the level of certification activities required when changes are made to the configuration of DOEHRS-DR 1.5.1
- c. If the PO deems the changes to the configuration to be “minor”, the changes can be documented using Release Notes that have a security section. An example of a “minor” change would be the addition of functional changes that do not make any changes to the security policies and procedures.
 - 1) If the PO deems the changes to the configuration to be more than “minor” but still less than a “major” change, a Risk Assessment must be coordinated with and validated by the JMISO Certification Team. The results normally will be documented as an addendum to the system accreditation report. An example of this type of change would be the addition of a new Commercial-Off-The-Shelf (COTS) product to the application or, adding one or more new interfaces to the system.
 - 2) If the PO deems the changes to the configuration to be a “major” change, a full Certification and Accreditation effort that leads to an Approval to Operate (ATO) must be performed by the JMISO Certification Team. Examples of “major” changes include changing the operating system, or changing a major component, such as the database used by the system.
- d. Mitigation of any of the system’s technical risks, identified under “Specific Conditions”, below, is not to be delayed for the duration of the approved certification, but rather completed by the PO as quickly as resources permit.

2. Specific Conditions:

- Take all necessary actions to close the Medium risk indicated in this report, or reduce this risk to a Low rating and to the extent that they may be considered an acceptable residual risk to the operation of DOEHRS-DR 1.5.1. The JMISO Certification Team and PO will coordinate efforts, prior to 01 December 2004, to allow JMISO verification that this task is completed

For Official Use Only

- Establish and document a procedure to ensure that the DOEHRS-DR 1.5.1 System Security Authorization Agreement (SSAA), including Appendices, is reviewed and updated as necessary upon any significant change to the system security or configuration and, at least, on an annual basis. DOEHRS-DR 1.5.1 will validate this action to the JMISO Certification Team prior to 01 December 2004
- Initiate efforts to establish an alternate site for DOEHRS-DR 1.5.1 at a location physically separate from APG in Aberdeen, Maryland

3. Other:

Best practices and JMISO policy will require DOEHRS-DR 1.5.1 to resolve any relevant issues relating to the upcoming discontinuation of Microsoft support of Windows NT. Although not considered a risk for the purposes of this Certification and Accreditation, these circumstances create a business risk because systems will be removed from Service networks if Windows NT is running and unsupported.

It is required that the aforementioned conditions be satisfied prior to the next Annual Review, unless a specific date is designated in a condition.