



DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
LANGLEY AIR FORCE BASE, VIRGINIA

30 NOV 2004

MEMORANDUM FOR HQ ACC/CE

FROM: HQ ACC/SC-2

SUBJECT: ACC Certificate to Operate (CtO) and Accreditation for Integrated Pest Management Information System (IPMIS) version 3.0

1. In accordance with AFPD 33-2, *Information Protection* and ACCI 33-174, *Certifying the ACC Enterprise*, I approve the operation of Integrated Pest Management Information System (IPMIS) version 3.0 for three years from the date of this letter and issue both a CtO and Accreditation. This approval allows the system to operate at all ACC bases up to the sensitive unclassified level in the system high security mode of operation. The Designated Approving Authority's (DAA) review of the Systems Security Authorization Agreement (SSAA) verifies that some system security countermeasures have been implemented, and an acceptable level-of-protection exists.
2. The assigned Information Systems Security Officer (ISSO) is required to follow the SSAA and DAA provided guidance throughout the life cycle of the system. The ACC Network Operations and Security Center will inform the local Network Control Center that the system is authorized for use on the ACC Enterprise. Before system activation, the functional information system's owner and the host Wing Information Assurance Office will complete the ACC Site Certification Checklist. The ISSO maintains the completed checklist and SSAA for the system's life cycle.
3. An automatic or cursory extension of an Accreditation will not be given beyond the expiration date of this approval. During this period, you must ensure appropriate actions are taken to address residual risks. Failure to mitigate the risks may prohibit use of the application beyond the date of this approval. An ACC/SCS Information Technology (IT) consultant will continue to work with your staff to develop a corrective action plan to resolve any remaining risks.
4. This CtO and Accreditation is only valid for the current version's system software configuration and associated hardware. Any changes to this system (i.e., revisions,

Global Power For America

upgrades, or new versions) will nullify this approval. Please contact your ACC/SCS IT consultant, Ms Patricia Oller, HQ ACC/SCSO, DSN 574-5885, if you have any questions.

A handwritten signature in black ink, appearing to read "Roland N. Lesieur". The signature is written in a cursive, flowing style.

**ROLAND N. LESIEUR, Colonel, USAF**

**Deputy Director**

**Communications and Information Systems**

**Detailed Risk Breakdown  
for  
IPMIS 3.0**

**1. Risks with No Countermeasures:**

**a. Risk:** “Users are DoD personnel worldwide and foreign nationals” (SSAA section 1.3.4, page 6). Foreign nationals associated with the vendor site are unknown and not within control of DoD.

(1) Impact: These foreign nationals could have indirect access inside ACC base firewalls.

(2) Corrective Measure(s): Download application only from a trusted source where it can be scanned and tested before being loaded to users’ workstations. This is enforceable through the NOSC/NCC using Smartfilter (CITS) to block the specific URLs that enable downloads (<http://www.envirosoftinc.com/IPMIS23/downloads> and <http://www.envirosoftinc.com/IPMIS30/downloads> ) while still allowing users to visit the website for other purposes.

(3) Limiting Factor: .exe files are currently blocked by NCCs, which is a deterrent

(3) Recommendation: Acceptable with corrective measure.

**b. Risk:** 2 main Servers are located at the vendor site, located at the University of Illinois.

(1) Impact: Potential for malicious code to be inserted in software and downloaded to the ACC Enterprise. Vendor site has no requirement for security clearance of personnel.

(2) Corrective Measure: Download application only from a trusted source where it can be scanned and tested before being loaded to users’ workstations. This is enforceable through the NOSC/NCC using Smartfilter (CITS product) to block the specific URLs that enable downloads (<http://www.envirosoftinc.com/IPMIS23/downloads> and <http://www.envirosoftinc.com/IPMIS30/downloads> ) while still allowing users to visit the website for other purposes.

(3) Limiting Factor: This risk is considered significant because malicious code in the form of viruses and worms often originate from academic environments. Personnel controls do exist at the vendor site in the form of locked doors and discretionary access control on the servers. Within ACC, a minimum of a Favorable NAC is required for access to the unclassified network.

(3) Recommendation: Acceptable with corrective measure.

**c. Risk:** “Rollup Tool” is identified in the diagram provided at illustration 3.4 in the SSAA, but its function is not described.

(1) Impact: IPMIS could be doing something that is not documented in the SSAA and DAA could be accepting risk that is unidentified.

(2) Corrective Measure: No “push” or “pull” of data should occur directly between the client and the vendor site. Download application only from a trusted source where it can be scanned and tested before being loaded to users’ workstations. This is enforceable through the NOSC/NCC using Smartfilter (CITS product) to block the specific URLs that enable downloads (<http://www.envirosoftinc.com/IPMIS23/downloads> and <http://www.envirosoftinc.com/IPMIS30/downloads> ) while still allowing users to visit the website for other purposes.

(3) Recommendation: Acceptable with corrective measure.

## **2. Risks with Insufficient Countermeasures:**

**a. Risk:** SSAA does not specify who controls creation of accounts and userIDs

(1) Impact: Potential users are not instructed on proper procedures to obtain and account and password.

(2) Corrective Measure: SSAA should clearly define responsibilities and POCs.

(3) Limiting Factor: SSAA does specify good password policy, password aging, etc.

(4) Recommendation: Acceptable.

## **3. Mitigated Risks:**

**a. Risk:** POCs are not sufficiently identified

(1) Impact: Users will not know who to contact for incident response, etc.

(2) Corrective Measure: While ideally this should be done from the AF level, bases may supply information in these areas that are appropriate to their individual locations. The checklist included with the approval will call for this information.

(3) Recommendation: Acceptable with corrective measure.

**b. Risk:** SSAA specifies Windows NT as the operating system of preference

(1) Impact: NT is no longer standard within ACC

(2) Corrective Measure: IPMIS will work on Windows 2000 or XP, documentation should be updated to reflect that.

(3) Recommendation: Acceptable.

## SITE CERTIFICATION CHECKLIST

IPMIS 3.0

	Completed	N/A
<b>Site Security Personnel</b>		
1. Identify Local Certification Authority.		
2. Notify Wing Information Assurance Office of impending installation.		
3. Assign other system security officials, (i.e. ISSO, SA, FSA, ...) and document in writing.		
<b>Documentation</b>		
1. Ensure local personnel possess a copy of the Certificate to Operate (CtO) package to include SSAA, DAA letter, and Breakdown of Residual Risks.		
2. Install AIS or application as described in the CtO package.		
3. Document a list of all hardware variances. If there are variances do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA		
4. Document a list of all software variances. If there are variances, do not implement until a change request is validated by the Certifying Authority and is approved by MAJCOM DAA		
5. Include a diagram of the system network if adding systems. Submit diagram with completed checklist.		
6. Document any site-specific security policies that are not already in the System Security Policy. If there are changes to the security policies do not implement until a change request is validated by the Certifying Authority and approved by MAJCOM DAA.		
7. Document any site-specific additions/deletions to the Threat/Vulnerability Matrix.		
<b>Certification</b>		
1. Perform any countermeasures identified in Risk Analysis section of SSAA and ACC Breakdown of Residual Risk.		
2. Verify system integrity by running an ISS scan. Correct and identify any additional vulnerabilities.		
3. If the AIS connects two or more different security classification networks, it must use an approved Secret and Below Interoperability (SABI) solution and receive final SABI board approval before operational use.		
4. Return this completed checklist to SCS.		
<b>Software Licensing</b>		
1. Ensure unit ISSO maintains a locatable copy of software license agreement per seat		
2. Ensure ISSO monitors compliance with the software license agreement		

**Certification Authority's Validation**

**Date Submitted:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_