



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

31 Jan 05

MEMORANDUM FOR HQ ACC/DO

FROM: HQ ACC/SC

SUBJECT: Certificate to Operate (CtO) and Approval to Operate (AtO) Very Small Aperture Terminal 2.5

1. In accordance with AFPD 33-2, *Information Protection* and ACCI 33-174, *Certifying the ACC Enterprise*, I approve the operation of Very Small Aperture Terminal 2.5 for 3 years from the date of this memorandum and issue both a CtO and AtO. This CtO and AtO allow 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 sufficient 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. This CtO and AtO are only valid for the current version's system software configuration and associated hardware. Any changes to this system (i.e., revisions, upgrades, or new versions) will nullify this approval. Please contact your ACC/SCS IT consultant, Mr. William Benson, HQ ACC/SCSO, DSN 575-2442, if you have any questions.

ROLAND N. LESIEUR, Colonel, USAF
Deputy Director
Communications and Information Systems

Attachments:

1. Risk Details
2. ACC Site Certification Checklist

SITE CERTIFICATION CHECKLIST
VSAT 2.5

	Completed	N/A
Site Security Personnel		
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.		
Documentation		
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.		
Certification		
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.		
Software Licensing		
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: _____

**Detailed Risk Breakdown
for
Very Small Aperture Terminal (VSAT) 2.5**

1. Risks with No Countermeasures:

None

2. Risks with Insufficient Countermeasures:

None

3. Mitigated Risks:

a. Risk: File Transfer Protocol (FTP) operates on TCP ports 20 and 21. FTP provides the capability to transfer files between hosts. User authentication is handles via a user name and a corresponding password. There is an optional facility to relax user authentication by way of the user name “anonymous” and an arbitrary password.

(1) **Impact:** Could allow an intruder to deliver unwanted files containing malicious software or contraband, the possibility of denial of service because of a full disk, or the interception of valid user names and passwords via network sniffing. An attacker could observe a valid user name and password via a sniffing attack and use the information for subsequent access. Data obtained via FTP poses the same risks as any data transferred via the Internet, particularly data-driven attacks.

(2) **Corrective Measure(s):** Allow inbound FTP to traverse the security perimeter using strong user authentication, and unrestricted outbound FTP.

(3) **Recommendation:** Acceptable with countermeasure.