



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

06 OCT 2003

MEMORANDUM FOR HQ ACC/DO

FROM: HQ ACC/SC

SUBJECT: Interim Approval to Operate and Interim Certificate to Operate for Portable Flight Planning Software (PFPS) Version 3.2 on Windows XP

1. In accordance with AFPD 33-2, *Information Protection*, I approve the operation of PFPS 3.2 for 1 year from the date of this letter and issue an Interim Approval to Operate (IAto) and an Interim Certificate to Operate (ICto). This approval allows the system to operate at all ACC bases up to the Top Secret Collateral 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. This approval is for the collateral components of PFPS only. No approval for SAP/SAR (Special Access Program/Special Access Required) is herein made nor should any such approval be inferred.
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. Program office is responsible for providing a C4I Support Plan and obtaining a Certificate of Networthiness from AFCA. 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 Interim Approval to Operate is 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 the IT Consultant Branch, HQ ACC/SCSO, 764-8356, if you have any questions.

A handwritten signature in black ink that reads "Roland N. Lesieur".

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

Attachments:

1. HQ ACC/SCSC Memo
2. ACC Site Certification Checklist



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

29 Sep 03

MEMORANDUM FOR HQ ACC/SC

FROM: HQ ACC/SCSC

SUBJECT: Recommendation for an ACC Interim Certificate to Operate (ICtO) and Interim Approval to Operate (IAtO) for Portable Flight Planning Software (PFPS) version 3.2 (on Windows XP)

1. PFPS 3.2 is a PC/Windows-based mission planning software suite that is capable of operating on a wide range of desktop and portable/laptop PC's. PFPS supports the mission planning needs for the United States Air Force, Air Force Special Operations Command (AFSOC) and United States Navy, providing automated mission planning, materials preparation, and post-mission debriefing capabilities. PFPS supports interfaces to intelligence and operation networks, and provides the capability to prepare and maintain data from external sources, as needed, to support the mission planning process.
2. There were numerous risks identified in the evaluation of the previous version of PFPS (3.1.2) in the Jun 02 IAtO. The main risks were associated with the reliance of PFPS on Air Force Mission Support System (AFMSS). The risks associated with the Jun 02 IAtO have not been sufficiently remedied or eliminated with this new version. After complete review and evaluation of the certification package, we recommend a one year ICtO and IAtO for PFPS version 3.2 in the system high security mode of operation up to the TOP SECRET level. This will give the PMO time to update the SSAA. The SSAA also states that PFPS will use periods processing up to the TS/SAR level. This recommendation and the subsequent approval are for the collateral components of PFPS only, and no recommendation for SAP/SAR (Special Access Program/Special Access Required) is herein made nor should any such recommendation be inferred.
3. Areas of residual risk remain; which will require additional risk management measures before accreditation can be granted. All remaining risks can be grouped into three main categories, summarized below. A detailed breakdown of residual risk is attached.
 - a. Risks with No Countermeasures: These are all the risks without any realistic countermeasures available. There may be certain limitations and constraints imposed to help mitigate these risks to an acceptable level.
 - b. Risks with Insufficient Countermeasures: These are all the risks with countermeasures applied, however, the countermeasures do not fully mitigate the risk. Countermeasures to further reduce risk may be unavailable or not economically feasible.
 - c. Mitigated Risks: These risks are deemed to have been reduced to a level where they no longer pose a measurable risk to system operation. They were presented as risks in the system

Global Power For America

certification package (identified during the risk analysis process or security test and evaluation), however, applied countermeasures or imposed limitations and constraints nullify these risks.

A handwritten signature in black ink, appearing to read "Charles P. Young". The signature is fluid and cursive, with a large loop at the end.

CHARLES P. YOUNG, Major, USAF
Chief, IT Assessment Branch
Directorate, Communications and Information Systems

Attachment:
Detailed Risk Breakdown

**Detailed Risk Breakdown
for
Portable Flight Planning System 3.2
(On WinXP)**

1. Risks with No Countermeasures:

a. Risk: The ST&E Plan has not been executed. There is no formal ST&E report.

(1) **Impact:** Inability to evaluate adequacy of security testing. Without an ST&E Report, a thorough review of the security measures cannot be accomplished.

(2) **Corrective Measure(s):** Perform the St&E and provide the report.

(3) **Recommendation:** Acceptable for an interim accreditation – ST&E report required for full accreditation.

b. Risk: Incomplete System Security Authorization Agreement (SSAA).

(1) **Impact:** An interim accreditation can be given based on a review of the System Description, System Security Policy, Certification and Accreditation Plan, and System Security Architecture documents. The interim accreditation will then allow the system developer or program manager to perform a ST&E. Once the ST&E is completed, the ST&E report and Risk Analysis can be written.

(2) **Corrective Measure(s):** Complete the missing documents of the SSAA.

(3) **Limiting Factor(s):** The Risk Analysis (RA) documents the residual risk of the system after taking into account the results of the ST&E. The Trusted Facility Manual (TFM) provides the system administrator with instructions on how to securely run the system. The Security Features Users Guide (SFUG) instructs all users in the security features of the system. The RA, TFM, and SFUG are needed to ensure that the system operates securely.

(4) **Recommendation:** Acceptable for interim accreditation. A complete SSAA is required for full accreditation.

2. Risks with Insufficient Countermeasures:

a. Risk: The commercial-off-the-shelf (COTS) products were developed in an open environment without integrity features.

(1) **Impact:** There is the potential that system programmers may have inserted malicious code or macros during system development. Also, the systems may be altered during normal processing by a malicious user.

(2) Corrective Measure(s): Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the trusted computer base. The system should be designed with system integrity functionality, such as check sums.

(3) Recommendation: Acceptable for interim.

b. Risk: Susceptibility to software viruses due to lack of antiviral software.

(1) Impact: Viruses could impair system security or operational capability.

(2) Corrective Measure(s): Install antiviral software

(3) Limiting Factor(s): The overall threat of Windows XP-based viruses is high due to the large number of computer viruses targeted at Windows 2000 and Windows XP.

(4) Recommendation: Acceptable with the installation of antiviral software.

3. Mitigated Risks:

a. Risk: Potential to connect to a network at a different classification than the network.

(1) Impact: If PFPS exposes a higher classification to the network than the network is cleared for, security incident results which creates a denial of service problem while the lower of the two networks is purged of the higher classification of data. If PFPS is running at a lower security level than the network it interfaces with, the PFPS memory device must be permanently reclassified to the higher level and any data intended for the lower classified network would have to be manually entered.

(2) Corrective Measure(s): Limit connectivity during processing to accredited and similarly processing workstations.

(3) Recommendation: Acceptable for interim.

b. Risk: PFPS does not have the capability for user-unique account names and passwords

(1) Impact: Non-compliance with identification and authentication to the granularity of a single user.

(2) Countermeasure: Maintain manual log of users' times and actions

(3) Recommendation: Acceptable with countermeasure

c. Risk: Data Transfer Devices (DTDs) are unencrypted with up to TS data

(1) **Impact:** Unencrypted data will be particularly vulnerable in small portable DTDs that could be mishandled and end up in the hands of an unauthorized individual.

(2) **Countermeasure:** Make certain DTDs are appropriately marked with the highest classification contained on it and handle accordingly.

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

d. Risk: PFPS does not have the capability to generate and maintain an electronic audit trail.

(1) **Impact:** Non-compliance with audit requirement

(2) **Countermeasure:** Maintain manual records as directed in CONOPS

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

e. Risk: CONOPS says MAJCOMs are responsible for determining what kind of facility, physical security requirements, etc. are appropriate.

(1) **Impact:** End users won't be able to get direction from the CONOPs document itself and would end up wasting time trying to determine who to call.

(2) **Corrective Measure:** Edit CONOPs to be more directive in nature. Direct users to specific guides, regulations, etc. or be specific with instructions.

(3) **Limiting Factor:** Section 5 of the System Security Architecture addresses personnel and physical security issues appropriately.

(4) **Recommendation:** Acceptable for interim

SITE CERTIFICATION CHECKLIST

Portable Flight Planning System 3.2

	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.		
Certification Authority's Validation		
Date Submitted: _____		
Signature: _____		
Name: _____		
Title: _____		