

**Command/Installation/Activity:** \_\_\_\_\_

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

<b>REVIEWED AREA/ITEM</b>	<b>FP STATUS</b>			<b>REMARKS</b>
	YES	NO	NA	
<b>STANDARD #21 (CIO)</b> C2 Protect Integration and Training				
AR380-19 continuous opns assessment/analysis integrated in AT/FP plans?				
Adherence to/integration AR380-53 security monitoring, exploitation, penetration?				
C2 Protect and AR 25-XX components integrated into AT/FP Program?				
OPSEC?				
Physical security?				
Intelligence?				
ISS?				
Counter-deception?				

**NOTES:**

CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.

**Command/Installation/Activity:** \_\_\_\_\_

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

<b>REVIEWED AREA/ITEM</b>	<b>FP STATUS</b>			<b>REMARKS</b>
	YES	NO	NA	
Counter-PSYOPS?				
Network incidents reviewed and trends developed indicating weaknesses?				
C2 Protect representative active on command AT/FP committee?				
System administrator incident reporting procedures, IAW AR380-19?				
Warning system devised to alert command to incidents?				
Command familiar with roles of LIWA/ACERT?				
OPSEC plan includes 530-1 provisions, threats ID'ed, OPSEC training?				
C2 Protect components in threat briefs, assessments for the command?				
Is there a computer security awareness program?				

**NOTES:**

CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.

**Command/Installation/Activity:** \_\_\_\_\_

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

<b>REVIEWED AREA/ITEM</b>	<b>FP STATUS</b>			<b>REMARKS</b>
	YES	NO	NA	
Command monitors C2P integration effectiveness at subordinate levels?				
System, network administrators trained, IAW AR 380-19?				
Does available training meet program requirements?				
Training plan to ensure continual operations during major disruptions?				
All persons trained, familiar w/OPSEC responsibilities, IAW AR 530-1?				
Appropriate security personnel appointed and trained (ISSO or NSO)?				

**NOTES:**

CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.

**Command/Installation/Activity:** \_\_\_\_\_

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

<b>REVIEWED AREA/ITEM</b>	<b>FP STATUS</b>			<b>REMARKS</b>
	<b>YES</b>	<b>NO</b>	<b>/ NA</b>	
<b>STANDARD #22</b> C2 Protect Threat and Vulnerability Assessments				
Registered in terminal Server Access Controller System for Army tool set access?				
Requirements for tools identified?				
ACERT incident reporting procedures in place and incidents reported?				
Do all administrators receive DISA Incident Support Team Bulletins?				
OPSEC process used to ID threats, vulnerabilities to communications systems?				
ISS procedures routinely reviewed and tested?				
ISS training performed at appropriate levels?				
Security incidents/violations (virus, unauthorized entry attempt, password compromise)				

**NOTES:**

CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.

**Command/Installation/Activity:** \_\_\_\_\_

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

		<b>FP STATUS</b>			
<b>REVIEWED AREA/ITEM</b>	<b>YES</b>	<b>NO</b>	<b>/</b>	<b>NA</b>	<b>REMARKS</b>
Analyzed, reviewed, investigated?					
Reported IAW AR 380-19, AR 25-XX and ACERT procedures?					
Security measures employed to control external access?					
Do all systems use an automated audit capability (to log security related events)?					
Identification and authentication required to enter all systems?					
OPSEC process applied in countermeasure development for communications structure?					
Army Communications infrastructure vulnerability assessments done?					
By authorized Army activities/approved contractors using US citizens only?					
Countermeasures identified, in place, based on vulnerability assessments?					

**NOTES:**

**CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.**

**Command/Installation/Activity:** \_\_\_\_\_

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

<b>REVIEWED AREA/ITEM</b>	<b>FP STATUS</b>			<b>REMARKS</b>
	YES	NO	NA	
Is there a written security plan to document implementation of countermeasures?				
Are sufficient secure communications available to the command?				

**NOTES:**  
CIO has primary responsibility, but takes input from all areas for evaluation of the FP Standard.