## Declassified and Approved For Release 2012/10/05 : CIA-RDP89B01354R000500640020-5

SAFEGUARD   APPLICABILITY   DOABLE WITH FY 85 MONEY   BY FY 90	COMPUSEC CRITICAL SYSTEMS: SAFEGUARDS APPLICABILITY				
Safeguard 1:       Mandatory Access Control       7       3       3         Safeguard 2:       Discretionary Access Control       10       7       8         Safeguard 3:       Object Reuse       9       4       9         Safeguard 4:       Labels       7       3       4         Safeguard 5:       Label Integrity       7       3       4         Safeguard 6:       Exportation of Labeled Information       7       3       4         Safeguard 7:       Exportation to Multilevel Devices       7       3       4         Safeguard 8:       Exportation to Single-Level Devices       6       2       3         Safeguard 9:       Labeling Human-Readable Output       8       3       3         Safeguard 10:       Subject Sensitivity Levels       5       2       2         Safeguard 11:       Device Levels       7       3       3         Safeguard 12:       Identification and Authentication       9       3       3         Safeguard 13:       Trusted Path       10       3       3         Safeguard 14:       Audit       1       3       3         Safeguard 15:       System Integrity       11       4       2	SAFECIIARD	APPLICABILITY	DOABLE WITH FY 85 MONEY		
Safeguard 2:       Discretionary Access Control       10       7       3       9       4       9       9       4       4       8       3       4       2       2       3 <td></td> <td>7</td> <td>3</td> <td>3</td>		7	3	3	
Safeguard 2:       Discretionary Access Control       9       4       9         Safeguard 3:       Object Reuse       7       3       4         Safeguard 4:       Labels       7       3       4         Safeguard 5:       Label Integrity       7       3       4         Safeguard 6:       Exportation of Labeled Information       7       3       4         Safeguard 7:       Exportation to Multilevel Devices       7       3       4         Safeguard 8:       Exportation to Single-Level Devices       6       2       3         Safeguard 9:       Labeling Human-Readable Output       8       3       3         Safeguard 10:       Subject Sensitivity Levels       5       2       2         Safeguard 11:       Device Levels       7       3       3         Safeguard 12:       Identification and Authentication       9       3       3         Safeguard 13:       Trusted Path       10       3       3         Safeguard 14:       Audit       1       3       3         Safeguard 15:       System Architecture       7       0       0         Safeguard 17:       Covert Channel Analysis       10       1       1		10	7	8	
Safeguard 4: Labels       7       3       4         Safeguard 5: Label Integrity       7       3       4         Safeguard 6: Exportation of Labeled Information       7       3       4         Safeguard 7: Exportation to Multilevel Devices       7       3       4         Safeguard 8: Exportation to Single-Level Devices       6       2       3         Safeguard 9: Labeling Human-Readable Output       8       3       3         Safeguard 10: Subject Sensitivity Levels       5       2       2         Safeguard 11: Device Levels       7       3       3         Safeguard 12: Identification and Authentication       9       3       3         Safeguard 13: Trusted Path       10       3       3         Safeguard 14: Audit       11       3       3         Safeguard 15: System Architecture       7       0       0         Safeguard 17: Covert Channel Analysis       10       1       1         Safeguard 18: Trusted Facility Management       8       3       3         Safeguard 19: Security Testing       10       7       7         Safeguard 20: Design Specification       8       2       2		9	4	9	
Safeguard 5: Label Integrity 7 3 4 4 5 5 5 4 5 5 5 5 5 5 5 5 5 5 5 5 5		. <i>7</i>	3	4	
Safeguard 6: Exportation of Labeled Information  Safeguard 7: Exportation to Multilevel Devices  Safeguard 8: Exportation to Single-Level Devices  Safeguard 9: Labeling Human-Readable Output  Safeguard 10: Subject Sensitivity Levels  Safeguard 11: Device Levels  Safeguard 12: Identification and Authentication  Safeguard 13: Trusted Path  Safeguard 14: Audit  Safeguard 15: System Architecture  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 20: Design Specification  Safeguard 20: Design Specification  Safeguard 20: Design Specification		,	3	4	
Safeguard 7: Exportation to Multilevel Devices 7 Safeguard 8: Exportation to Single-Level Devices 6 Safeguard 9: Labeling Human-Readable Output 8 Safeguard 10: Subject Sensitivity Levels 5 Safeguard 11: Device Levels 7 Safeguard 12: Identification and Authentication 9 Safeguard 13: Trusted Path 10 Safeguard 14: Audit 11 Safeguard 15: System Architecture 7 Safeguard 16: System Integrity 11 Safeguard 17: Covert Channel Analysis 10 Safeguard 18: Trusted Pacility Management 8 Safeguard 19: Security Testing 10 Safeguard 20: Design Specification 8		, -	3	4	
Safeguard 8: Exportation to Single-Level Devices  Safeguard 9: Labeling Human-Readable Output  8 Safeguard 10: Subject Sensitivity Levels  5 Safeguard 11: Device Levels  7 Safeguard 12: Identification and Authentication  9 Safeguard 13: Trusted Path  10 3 Safeguard 14: Audit  Safeguard 15: System Architecture  7 Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  8 Safeguard 19: Security Testing  Safeguard 20: Design Specification  8  3  3  3  3  3  3  3  3  3  3  3  3		. /	3	4	
Safeguard 9: Labeling Human-Readable Output 8 Safeguard 10: Subject Sensitivity Levels 5 Safeguard 11: Device Levels 7 Safeguard 12: Identification and Authentication 9 Safeguard 13: Trusted Path 10 Safeguard 14: Audit 11 Safeguard 15: System Architecture 7 Safeguard 16: System Integrity 11 Safeguard 17: Covert Channel Analysis 10 Safeguard 18: Trusted Facility Management 8 Safeguard 19: Security Testing 10 Safeguard 20: Design Specification 8		. 7		3	
Safeguard 9: Labeling Human-Readable Output  Safeguard 10: Subject Sensitivity Levels 5  Safeguard 11: Device Levels 7  Safeguard 12: Identification and Authentication 9  Safeguard 13: Trusted Path 10  Safeguard 14: Audit 11  Safeguard 15: System Architecture 7  Safeguard 16: System Integrity 11  Safeguard 17: Covert Channel Analysis 10  Safeguard 18: Trusted Facility Management 8  Safeguard 19: Security Testing 10  Safeguard 20: Design Specification 8	Safeguard 8: Exportation to Single-Level Devices	6	2	3	
Safeguard 10: Subject Sensitivity Levels  Safeguard 11: Device Levels  7  Safeguard 12: Identification and Authentication  Safeguard 13: Trusted Path  Safeguard 14: Audit  Safeguard 15: System Architecture  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  Safeguard 20: Design Specification	Safeguard 9: Labeling Human-Readable Output	8	3	2	
Safeguard 11: Device Levels  Safeguard 12: Identification and Authentication  Safeguard 13: Trusted Path  Safeguard 14: Audit  Safeguard 15: System Architecture  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  7  3  3  3  3  3  3  3  3  3  3  3  3		5	2	2	
Safeguard 12: Identification and Authentication  Safeguard 13: Trusted Path  Safeguard 14: Audit  Safeguard 15: System Architecture  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  9 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		7	3	, .J	
Safeguard 13: Trusted Path  Safeguard 14: Audit  Safeguard 15: System Architecture  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  10  3  3  3  3  4  2  5  5  6  7  7  7  7  8  8  9  9  9  9  9  9  9  9  9  9  9	Safeguard 12: Identification and Authentication	9	3	3	
Safeguard 14: Audit  Safeguard 15: System Architecture  7  Safeguard 16: System Integrity  Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  8  3  3  3  3  3  3  3  3  3  3  3  3		10	3	3	
Safeguard 15: System Architecture 7 Safeguard 16: System Integrity 11 Safeguard 17: Covert Channel Analysis 10 Safeguard 18: Trusted Facility Management 8 Safeguard 19: Security Testing 10 Safeguard 20: Design Specification 8 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		11	3	,	
Safeguard 16: System Integrity 11 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		7	0	0	
Safeguard 17: Covert Channel Analysis  Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  8  2  3  3  3  3  3  3  3  3  3  3  3  3	·	11	4	2	
Safeguard 18: Trusted Facility Management  Safeguard 19: Security Testing  Safeguard 20: Design Specification  8  2  3  3  3  3  3  3  3  3  3  3  3  3		10	1 "	<u> </u>	
Safeguard 19: Security Testing 10 7 Safeguard 20: Design Specification 8 2 2 3		8	3	· · · . 3	
Safeguard 20: Design Specification 8 2		10	7	· . 7	
		8	2	2	
<b>₹</b>	Safeguard 21: Configuration Management	11	3	3	

<sup>\*\*</sup>Numbers represent the total of 11 Critical Systems

Declassified and Approved For Release 2012/10/05 : CIA-RDP89B01354R000500640020-5

	COMPUSEC CRITICAL SYSTEM	S: SAFEGUARDS AF	PPLICABILITY	, ,
SAFEC	SUARD	APPLICABILITY	DOABLE WITH FY 85 MONEY	TECH. FEASIBL
	:			
Safeguard 22:	System Security Plan	11	11	11
Safeguard 23:	External Marking of Removable Storage Media	11	11	11
Safeguard 24:	Intelligent Terminals and Personal Computers	11	11	11
Safeguard 25:	Clearance of Maintenance Personnel	11	6	6
Safeguard 26:	Annual Accreditation Requirement	11	11	11
Safeguard 27:	Accreditation Authority for Automated Message Processing Systems	7	7	7
Safeguard 28:	Accreditation of Automated Message Handling Systems	. 7	i.7	. 7
Safeguard 29:	Accreditation Recording	11	11 ·	11
Safeguard 30:	Control Mechanisms in Automated Message Handling Systems	5	3	4
Safeguard 31:	Automated Message Handling System Auditing Capabilities	5 .	3	4
Safeguard 32:	Prohibition on Use of Unencrypted and Dial-up Lines	11	10	10
Safeguard 33:	Protection of Security-Related Software	11	3	3
Safeguard 34:	Separation of Duties	10	10	10
Safeguard 35:	Access Authorization Approvals	11	10	10
Safeguard 36:	Awareness of and Compliance with Appropriate Security Policies (including training)	11 .	11	10
Safeguard 37:	Two Independent Access Authorization Mechanisms	4	3	3
Safeguard 38:	Physical Security	11	11	11
Safeguard 39:	Personnel Security	11	10	. 10
Safeguard 40:		11	10 .	10
		11	. 11	11