CSEC CRITERIA TO SCI POLICY COMPARISON MATRICES

31 OCT 84

First - Matrix pattern:

Evaluation of the level at which matching criteria satisfy the SCI polcy requirements for both Systems High Mode and Compartmented Mode of Operation, both before and after DIA's formal comments to the criteria are applied. The following legend is used:

LEGEND

U - unacceptable

F - unacceptable due to correctable flow

M - minimally acceptable under some conditions

A - acceptable

S - stronger than needs to be, but reasonable

O - over protected in comparison to requirement

E - excessive protection

Second - Matrix pattern:

Comparison of whether corresponding criteria exist for SCI policy requirements for both System High Mode and Compartmented Mode of Operation, both before and after DIA's formal comments to the criteria are applied.

Third - Matrix pattern:

Display of full set of criteria and correspondence to SCI policy requirements for both System High and Compartmented Modes of Operation, both before and after DIA's formal comments are applied.

REQUIREMENTS SATISFACTION BEFORE DIA COMMENTS
CSEC CRITERIA AND SCI SYSTEM HIGH MODE

18 June 1984

SYSTEM HIGH MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	F	F	F	F	F	CHAPTER 2, 2.f.(5).
+OBJECT REUSE	A	A	A	A	-	NOT REQUIRED
LABELS	S	S	A	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	S	S	S	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	O	O	O	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	S	S	S	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	S	S	-	-	-	NOT REQUIRED
DEVICE LABELS	S/A	S/A	-	-	-	REQUIREMENT 8 (remote terminals)
IDENTIFICATION AND AUTHENTICATION	O	O	O	A	U	REQUIREMENTS 8, 10
AUDIT	O	O	S	M	-	REQUIREMENT 15
+SYSTEM ARCHITECTURE	E	E	S	A	U	NOT REQUIRED
SYSTEM INTEGRITY	A	A	A	A	A	CHAPTER 3
TRUSTED FACILITY MANAGEMENT	A	M	-	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	E	O	S	A	M	CHAPTER 3, 3.b.
CONFIGURATION MANAGEMENT	O/F	O/F	-	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	A	A	A	A	A	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	E	E	O	A	U	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	O	O	A	A	A	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	E	E	S	A	A	CHAPTER 3, 2.

\+ Required by practice for new systems rather than policy documents.

++ Desirable on all systems at level C3 and above.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

REQUIREMENTS SATISFACTION AFTER DIA COMMENTS
CSEC CRITERIA AND SCI SYSTEM HIGH MODE

31 Oct 1984

SYSTEM HIGH MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	S	A	A	A	A	U	CHAPTER 2, 2.f.(5).
+OBJECT REUSE	A	A	A	A	A	A	NOT REQUIRED
LABELS	S	S	A	A	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	S	S	S	A	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	0	0	0	A	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	S	S	S	A	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	S	S	-	-	-	-	NOT REQUIRED
DEVICE LABELS	S/A	S/A	A	A	-	-	REQUIREMENT 8 (remote terminals)
IDENTIFICATION AND AUTHENTICATION	0	0	0	A	A	U	REQUIREMENTS 8, 10
AUDIT	0	0	S	A	M	-	REQUIREMENT 15
+SYSTEM ARCHITECTURE	E	E	S	A	A	U	NOT REQUIRED
SYSTEM INTEGRITY	A	A	A	A	A	A	CHAPTER 3
TRUSTED FACILITY MANAGEMENT	A	A	A	A	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	E	0	S	A	A	M	CHAPTER 3, 3.b.
CONFIGURATION MANAGEMENT	0/F	0/F	A	A	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	A	A	A	A	A	A	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	E	E	0	A	A	U	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	0	0	A	A	A	A	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	E	E	S	A	A	A	CHAPTER 3, 2.

\+ Required by practice for new systems rather than policy documents.

++ Desirable on all systems at level C3 and above.

NOTE: **C3 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

REQUIREMENTS SATISFACTION BEFORE DIA COMMENTS
CSEC CRITERIA AND SCI COMPARTMENTED MODE

31 Oct 1984

COMPARTMENTED MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	F	F	F	F	F	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	A	A	A	A	-	REQUIREMENT 13
LABELS	S	S	A	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	A	A	A	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	A	A	A	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	A	A	A	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	S	S	-	-	-	NOT REQUIRED
DEVICE LABELS	S/A	S/A	-	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	O/S/F	O/S/F	S/F	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	A	A	A	U	U	REQUIREMENTS 8, 10
AUDIT	O	O	S	U	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	E	O/S	A	M	U	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	A	A	A	A	A	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
TRUSTED FACILITY MANAGEMENT	A	U	-	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	E/O	O/S	A/S	M	U	CHAPTER 3, 3.b.
++DESIGN SPECIFICATION AND VERIFICATION	E/O	O	S	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	S/F	S/F	-	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	A	A	A	A	A	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	S	S	A	M	U	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	O	O	A	A	A	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	E	E/O	A	M	M	CHAPTER 3, 2.

++ Desirable on all systems at level C3 and above.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**

REQUIREMENTS SATISFACTION AFTER DIA COMMENTS
CSEC CRITERIA AND SCI COMPARTMENTED MODE

31 Oct 1984

COMPARTMENTED MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	S	A	A	A	M	U	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	A	A	A	A	A	A	REQUIREMENT 13
LABELS	S	S	A	A	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	A	A	A	U	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	A	A	A	M	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	A	A	A	M	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	S	S	-	-	-	-	NOT REQUIRED
DEVICE LABELS	S/A	S/A	A	A	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	O/S	O/S	S	-	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	A	A	A	U	U	U	REQUIREMENTS 8, 10
AUDIT	O	O	S	A	U	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	E	O/S	A	M	M	U	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	A	A	A	A	A	A	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
TRUSTED FACILITY MANAGEMENT	A	A	A	A	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	E/O	O/S	A/S	M	M	U	CHAPTER 3, 3.b.
++DESIGN SPECIFICATION AND VERIFICATION	E/O	S	S	-	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	S/F	S/F	A	A	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	A	A	A	A	A	A	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	S	S	A	M	M	U	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	O	O	A	A	A	A	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	E	E/O	A	M	M	M	CHAPTER 3, 2.

++ Desirable on all systems at level C3 and above.

NOTE: **B1 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**

REQUIREMENTS COMPARISON BEFORE DIA COMMENTS
CSEC CRITERIA AND SCI SYSTEM HIGH MODE

18 June 1984

SYSTEM HIGH MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	CHAPTER 2, 2.f.(5).
+OBJECT REUSE	*	*	*	*	-	NOT REQUIRED
LABELS	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	*	*	*	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	*	*	-	-	-	NOT REQUIRED
DEVICE LABELS	*	*	-	-	-	REQUIREMENT 8 (remote terminals)
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	REQUIREMENTS 8, 10
AUDIT	*	*	*	*	-	REQUIREMENT 15
+SYSTEM ARCHITECTURE	*	*	*	*	*	NOT REQUIRED
SYSTEM INTEGRITY	*	*	*	*	*	CHAPTER 3
TRUSTED FACILITY MANAGEMENT	*	*	-	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	*	*	*	*	*	CHAPTER 3, 3.b.
CONFIGURATION MANAGEMENT	*	*	-	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	CHAPTER 3, 2.

\+ Required by practice for new systems rather than policy documents.

++ Desirable on all systems at level C3 and above.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

REQUIREMENTS SATISFACTION AFTER DIA COMMENTS
CSEC CRITERIA AND SCI SYSTEM HIGH MODE

31 Oct 1984

SYSTEM HIGH MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	CHAPTER 2, 2.f.(5).
+OBJECT REUSE	*	*	*	*	*	*	NOT REQUIRED
LABELS	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	*	*	-	-	-	-	NOT REQUIRED
DEVICE LABELS	*	*	*	*	-	-	REQUIREMENT 8 (remote terminals)
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	REQUIREMENTS 8, 10
AUDIT	*	*	*	*	*	-	REQUIREMENT 15
+SYSTEM ARCHITECTURE	*	*	*	*	*	*	NOT REQUIRED
SYSTEM INTEGRITY	*	*	*	*	*	*	CHAPTER 3
TRUSTED FACILITY MANAGEMENT	*	*	*	*	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	*	*	*	*	*	*	CHAPTER 3, 3.b.
CONFIGURATION MANAGEMENT	*	*	*	*	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 2.

\+ Required by practice for new systems rather than policy documents.

++ Desirable on all systems at level C3 and above.

NOTE: **C3 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

REQUIREMENTS COMPARISON BEFORE DIA COMMENTS
CSEC CRITERIA AND SCI COMPARTMENTED MODE

31 Oct 1984

COMPARTMENTED MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	*	*	*	*	-	REQUIREMENT 13
LABELS	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	*	*	*	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	*	*	-	-	-	NOT REQUIRED
DEVICE LABELS	*	*	-	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	REQUIREMENTS 8, 10
AUDIT	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	*	*	*	*	*	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
TRUSTED FACILITY MANAGEMENT	*	*	-	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	*	*	*	*	*	CHAPTER 3, 3.b.
++DESIGN SPECIFICATION AND VERIFICATION	*	*	*	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	*	*	-	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	CHAPTER 3, 2.

++ Desirable on all systems at level C3 and above.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**

REQUIREMENTS COMPARISON AFTER DIA COMMENTS
CSEC CRITERIA AND SCI COMPARTMENTED MODE

31 Oct 1984

COMPARTMENTED MODE SECURITY POLICY REQUIREMENTS	CRITERIA CONTENTS BY LEVEL B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	*	*	*	*	*	*	REQUIREMENT 13
LABELS	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	-	-	REQUIREMENT 11
LABELING HUMAN READABLE OUTPUT	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
++SUBJECT SENSITIVITY LABELS	*	*	-	-	-	-	NOT REQUIRED
DEVICE LABELS	*	*	*	*	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	-	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	REQUIREMENTS 8, 10
AUDIT	*	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	*	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	*	*	*	*	*	*	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
TRUSTED FACILITY MANAGEMENT	*	*	*	*	-	-	CHAPTER 3, 3.b.(4)
SECURITY TESTING	*	*	*	*	*	*	CHAPTER 3, 3.b.
++DESIGN SPECIFICATION AND VERIFICATION	*	*	*	-	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	*	*	*	*	-	-	CHAPTER 3, 3.b.(4).(d).
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 2.

++ Desirable on all systems at level C3 and above.

NOTE: **B1 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**

CSEC CRITERIA AND SCI SYSTEM HIGH MODE
BEFORE DIA COMMENTS

31 Oct 1984

CRITERIA CONTENTS BY LEVEL

CSEC CRITERIA	A1	B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	CHAPTER 2, 2.f.(5).
OBJECT REUSE	*	*	*	*	*	-	
LABELS	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	-	-	REQUIREMENT 11
TO SINGLE LEVEL DEVICES	*	*	*	*	-	-	
TO MULTI-LEVEL DEVICES	*	*	*	*	-	-	
LABELING HUMAN READABLE OUTPUT	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
SUBJECT SENSITIVITY LABELS	*	*	*	-	-	-	
DEVICE LABELS	*	*	*	-	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	*	-	-	ENCLOSURE 8
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	REQUIREMENTS 8, 10
TRUSTED PATH	*	*	*	-	-	-	
AUDIT	*	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	*	
SYSTEM INTEGRITY	*	*	*	*	*	*	CHAPTER 3
COVERT CHANNEL ANALYSIS	*	*	*	-	-	-	
TRUSTED FACILITY MANAGEMENT	*	*	*	-	-	-	CHAPTER 3, 3.b.(4)
TRUSTED RECOVERY	*	*	-	-	-	-	
SECURITY TESTING	*	*	*	*	*	*	CHAPTER 3, 3.b.
DESIGN SPECIFICATION AND VERIFICATION	*	*	*	*	-	-	
CONFIGURATION MANAGEMENT	*	*	*	-	-	-	CHAPTER 3, 3.b.(4).(d).
TRUSTED DISTRIBUTION	*	-	-	-	-	-	
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 2.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

CSEC CRITERIA AND SCI SYSTEM HIGH MODE
AFTER DIA COMMENTS

31 Oct 1984

CRITERIA CONTENTS BY LEVEL

CSEC CRITERIA	A1	B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	*	CHAPTER 2, 2.f.(5).
OBJECT REUSE	*	*	*	*	*	*	*	
LABELS	*	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	*	-	-	REQUIREMENT 11
TO SINGLE LEVEL DEVICES	*	*	*	*	-	-	-	
TO MULTI-LEVEL DEVICES	*	*	*	*	-	-	-	
LABELING HUMAN READABLE OUTPUT	*	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
SUBJECT SENSITIVITY LABELS	*	*	*	-	-	-	-	
DEVICE LABELS	*	*	*	*	*	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	*	-	-	-	ENCLOSURE 8
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	*	REQUIREMENTS 8, 10
TRUSTED PATH	*	*	*	-	-	-	-	
AUDIT	*	*	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	*	*	
SYSTEM INTEGRITY	*	*	*	*	*	*	*	CHAPTER 3
COVERT CHANNEL ANALYSIS	*	*	-	-	-	-	-	
TRUSTED FACILITY MANAGEMENT	*	*	*	*	*	-	-	CHAPTER 3, 3.b.(4)
TRUSTED RECOVERY	*	*	-	-	-	-	-	
SECURITY TESTING	*	*	*	*	*	*	*	CHAPTER 3, 3.b.
DESIGN SPECIFICATION AND VERIFICATION	*	*	*	*	-	-	-	
CONFIGURATION MANAGEMENT	*	*	*	*	*	-	-	CHAPTER 3, 3.b.(4).(d).
TRUSTED DISTRIBUTION	*	-	-	-	-	-	-	
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	*	CHAPTER 3, 2.

NOTE: **C3 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR SYSTEM HIGH MODE.**

CSEC CRITERIA AND SCI COMPARTMENTED MODE
BEFORE DIA COMMENTS

20 June 1984

CRITERIA CONTENTS BY LEVEL

CSEC CRITERIA	A1	B3	B2	B1	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	*	*	*	*	*	-	REQUIREMENT 13
LABELS	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	-	-	REQUIREMENT 11
TO SINGLE LEVEL DEVICES	*	*	*	*	-	-	
TO MULTI-LEVEL DEVICES	*	*	*	*	-	-	
LABELING HUMAN READABLE OUTPUT	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
SUBJECT SENSITIVITY LABELS	*	*	*	-	-	-	
DEVICE LABELS	*	*	*	-	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	*	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	REQUIREMENTS 8, 10
TRUSTED PATH	*	*	*	-	-	-	
AUDIT	*	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	*	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	*	*	*	*	*	*	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
COVERT CHANNEL ANALYSIS	*	*	*	-	-	-	REQUIREMENT 2, CHAPTER 3, 3.b.(5).
TRUSTED FACILITY MANAGEMENT	*	*	*	-	-	-	CHAPTER 3, 3.b.(4)
TRUSTED RECOVERY	*	*	-	-	-	-	
SECURITY TESTING	*	*	*	*	*	*	CHAPTER 3, 3.b.
DESIGN SPECIFICATION AND VERIFICATION	*	*	*	*	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	*	*	*	-	-	-	CHAPTER 3, 3.b.(4).(d).
TRUSTED DISTRIBUTION	*	-	-	-	-	-	
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	CHAPTER 3, 2.

NOTE: **B2 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**

CSEC CRITERIA AND SCI COMPARTMENTED MODE
AFTER DIA COMMENTS

31 Oct 1984

CRITERIA CONTENTS BY LEVEL

CSEC CRITERIA	A1	B3	B2	B1	C3	C2	C1	DIAM 50-4 REFERENCES
DISCRETIONARY ACCESS CONTROL	*	*	*	*	*	*	*	CHAPTER 2, 2.f.(5)., REQUIREMENTS 7, 14
OBJECT REUSE	*	*	*	*	*	*	*	REQUIREMENT 13
LABELS	*	*	*	*	*	-	-	REQUIREMENTS 8, 11
LABEL INTEGRITY	*	*	*	*	*	-	-	REQUIREMENT 11
EXPORTATION OF LABELED INFORMATION	*	*	*	*	*	-	-	REQUIREMENT 11
TO SINGLE LEVEL DEVICES	*	*	*	*	-	-	-	
TO MULTI-LEVEL DEVICES	*	*	*	*	-	-	-	
LABELING HUMAN READABLE OUTPUT	*	*	*	*	*	-	-	REQUIREMENT 11 (a),(b)
SUBJECT SENSITIVITY LABELS	*	*	*	-	-	-	-	
DEVICE LABELS	*	*	*	*	*	-	-	REQUIREMENT 8 (remote terminals)
MANDATORY ACCESS CONTROL	*	*	*	*	-	-	-	CHAPTER 2, 2.a.
IDENTIFICATION AND AUTHENTICATION	*	*	*	*	*	*	*	REQUIREMENTS 8, 10
TRUSTED PATH	*	*	*	-	-	-	-	
AUDIT	*	*	*	*	*	*	-	REQUIREMENT 15
SYSTEM ARCHITECTURE	*	*	*	*	*	*	*	REQUIREMENTS 1, 2, 3 ,12
SYSTEM INTEGRITY	*	*	*	*	*	*	*	REQUIREMENTS 4, 5, 6, 9, CHAPTER 3
COVERT CHANNEL ANALYSIS	*	*	-	-	-	-	-	REQUIREMENT 2, CHAPTER 3, 3.b.(5).
TRUSTED FACILITY MANAGEMENT	*	*	*	*	*	-	-	CHAPTER 3, 3.b.(4)
TRUSTED RECOVERY	*	*	-	-	-	-	-	
SECURITY TESTING	*	*	*	*	*	*	*	CHAPTER 3, 3.b.
DESIGN SPECIFICATION AND VERIFICATION	*	*	*	*	-	-	-	CHAPTER 3, 3.a.
CONFIGURATION MANAGEMENT	*	*	*	*	*	-	-	CHAPTER 3, 3.b.(4).(d).
TRUSTED DISTRIBUTION	*	-	-	-	-	-	-	
SECURITY FEATURES USER'S GUIDE	*	*	*	*	*	*	*	CHAPTER 3, 3.a.
TRUSTED FACILITY MANUAL	*	*	*	*	*	*	*	CHAPTER 3, 3.b.(4).(a).
TEST DOCUMENTATION	*	*	*	*	*	*	*	CHAPTER 3, 3.b.(5)., ENCLOSURE 7
DESIGN DOCUMENTATION	*	*	*	*	*	*	*	CHAPTER 3, 2.

NOTE: **B1 LEVEL MEETS MINIMUM SCI REQUIREMENTS FOR COMPARTMENTED MODE.**