

ISO/IEC 21827:2008-10 (E)

Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®)

Contents		Page
Foreword		v
0	Introduction	vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Background	6
4.1	Reason for Development	7
4.2	The Importance of Security Engineering	7
4.3	Consensus	7
5	Structure of the Document	8
6	Model Architecture	8
6.1	Security Engineering	8
6.2	Security Engineering Process Overview	11
6.3	SSE-CMM® Architecture Description	14
6.4	Summary Chart	22
7	Security Base Practices	23
7.1	PA01 Administer Security Controls	24
7.2	PA02 - Assess Impact	28
7.3	PA03 - Assess Security Risk	32
7.4	PA04 - Assess Threat	36
7.5	PA05 - Assess Vulnerability	39
7.6	PA06 - Build Assurance Argument	43
7.7	PA07 - Coordinate Security	46
7.8	PA08 - Monitor Security Posture	49
7.9	PA09 - Provide Security Input	54
7.10	PA10 - Specify Security Needs	59
7.11	PA11 - Verify and Validate Security	63
Annex A (normative) Generic Practices		67
Annex B (normative) Project and Organizational Base Practices		68
B.1	General	68
B.2	General Security Considerations	68
B.3	PA12 - Ensure Quality	69
B.4	PA13 - Manage Configurations	74
B.5	PA14 - Manage Project Risks	78
B.6	PA15 - Monitor and Control Technical Effort	82
B.7	PA16 - Plan Technical Effort	86
B.8	PA17 - Define Organization's Systems Engineering Process	92
B.9	PA18 - Improve Organization's Systems Engineering Processes	96
B.10	PA19 - Manage Product Line Evolution	99
B.11	PA20 - Manage Systems Engineering Support Environment	102

B.12	PA21 - Provide Ongoing Skills and Knowledge	106
B.13	PA22 - Coordinate with Suppliers	112
Annex C (informative) Capability Maturity Model Concepts		117
C.1	General	117
C.2	Process Improvement	117
C.3	Expected Results	118
C.4	Common Misunderstandings	118
C.5	Key Concepts	120
Annex D (informative) Generic Practices		124
D.1	General	124
D.2	Capability Level 1 - Performed Informally	125
D.3	Capability Level 2 - Planned and Tracked	126
D.4	Capability Level 3 - Well Defined	132
D.5	Capability Level 4 - Quantitatively Controlled	137
D.6	Capability Level 5 - Continuously Improving	139
Bibliography		142