

Table of Contents

<u>PREFACE</u>	7
<u>SECURITY MODELS, THEORIES AND STANDARDS</u>	9
THE COMPUTER SYSTEM ITSELF AS LARGELY AN UNTRUSTED SYSTEM.....	9
DEFENSE IN DEPTH.....	9
VULNERABILITIES.....	10
SECURING SYSTEM AND DATA.....	17
SECURITY MEASURES.....	18
DESIGN PLANNING.....	20
<u>INFORMATION SECURITY PRACTICES</u>	21
IS MANAGEMENT ACTIVITIES.....	21
INFORMATION MANAGEMENT POLICY.....	22
ORGANIZATIONAL STRUCTURE AND SUPPORT.....	22
THE ROLE OF AN INFORMATION SECURITY PROFESSIONAL.....	23
IS CONTROL CLASSIFICATION.....	24
ACCESS CONTROL MODELS.....	26
ACLs VERSUS CAPABILITIES.....	27
WHAT IS ORANGE BOOK?.....	28
TYPES OF ACCESS CONTROL.....	28
THE AAA CONCEPT.....	29
PRACTICAL ACCESS CONTROL MEASURES.....	31
ESTABLISHING ACCOUNTABILITY THROUGH EVENT LOGGING.....	33
<u>PROTECTION OF INFORMATION ASSETS THROUGH SECURITY POLICIES AND MEASURES</u>	35
INFORMATION ASSETS.....	35
DATA CLASSIFICATIONS AND LAYER OF RESPONSIBILITIES.....	35
SECURITY POLICY.....	36
EFFECTIVE SECURITY PRACTICES.....	38
OWNERSHIP & RESPONSIBILITY.....	39
SECURITY AWARENESS TRAINING.....	40
SECURITY MODELS AND MODES OF OPERATIONS.....	41
EXAMPLE POLICY.....	42
CONSEQUENCES OF VIOLATIONS.....	43
EVALUATION.....	43
DEVISING YOUR OWN CLASSIFICATION SCHEME.....	43

TECHNICAL MANAGEMENT, ENGINEERING MANAGEMENT AND SECURITY ENGINEERING.....	44
CHANGE CONTROL.....	44
CONFIGURATION MANAGEMENT	45
<u>STANDARDS, GUIDELINES AND LAWS.....</u>	45
ISC2 VS ISACA.....	45
SoGP.....	46
ISO 17799.....	46
SARBANES–OXLEY ACT.....	46
THE COSO FRAMEWORK	47
FISMA	47
THE INFOSEC ASSESSMENT METHODOLOGY (IAM)	47
OCTAVE.....	48
FISMA	48
COMMON CRITERIA (CC).....	49
COMSEC & TEMPEST.....	49
NISPOM	50
ACCREDITATION AND CERTIFICATION	50
OTHER LAWS, STATUTES, AUTHORITIES AND REGULATIONS	51
<u>NETWORKING TERMINOLOGIES AND TECHNOTES.....</u>	52
REDUNDANCY AND/OR FALLBACK MEASURES	54
NETWORK INFRASTRUCTURE IMPLEMENTATION	54
OSI (OPEN SYSTEM INTERCONNECT)	55
LAN NETWORKING	55
ROUTING AND SWITCHING	57
IP ADDRESSING.....	58
NETWORK PROTOCOLS	59
WIRELESS BASED LOCAL AREA NETWORKING.....	60
WAN NETWORKING	61
TELECOMMUNICATION INFRASTRUCTURE.....	62
NETWORK SECURITY AND AVAILABILITY DEVICES.....	64
CRYPTOGRAPHY	65
DATABASE SECURITY	65
SYSTEM IMPLEMENTATION & MAINTENANCE.....	66
SPECIAL DEVICES AND TECHNOLOGIES.....	66
RFID	67
SERVICE-ORIENTED ARCHITECTURE	67
<u>SECURITY CERTIFICATION AND ACCREDITATION.....</u>	67

DEFINING ACCREDITATION AND CERTIFICATION.....	67
PHASES OF THE PROCESS	68
BOUNDARIES OF ACCREDITATION	69
OUTCOMES OF ACCREDITATION.....	69
DIACAP.....	70
DEFENSE IN DEPTH AND EAL.....	70
INFORMATION ASSURANCE AND THE IATF.....	71
SPONSORING ORGANIZATION MODEL.....	72

NISPOM IN DEPTH.....73

WHAT IS THE NISPOM FOR, AND WHO DEvised IT?.....	73
WHAT ARE THE LEVELS OF SECURITY CLEARANCES? WHO ADMINISTER SECURITY CLEARANCE? WHO CAN BE GRANTED CLEARANCES?.....	73
WHAT DETERMINES ACCESS TO CLASSIFIED INFORMATION?.....	74
CAN CLEARANCE BE GRANTED ON A TEMPORARY BASIS?.....	74
WHAT ARE THE VALID CLASSES OF INFORMATION?.....	74
WHAT ARE THE ROLES INVOLVED?	74
WHAT IF CLEARANCE IS NOT GRANTED? ANY EXCEPTIONS ALLOWED?	75
WHAT IS THE FSO REQUIREMENT?	75
WHAT ARE THE RESPONSIBILITIES OF THE CONTRACTORS?	75
WHAT ARE TO BE DONE WITH THE SECURITY REVIEWS, AND HOW ARE THEY DONE?.....	76
HOW TO HANDLE DUPLICATIVE SECURITY REVIEWS?	76
WHAT IS RISK MANAGEMENT, AND HOW DOES IT WORK?	76
WHAT KINDS OF EVENT MUST BE REPORTED?.....	77
WHO REVIEWS CLASSIFIED/UNCLASSIFIED REPORTS?.....	77
HOW DOES REPORT SUBMISSION WORK?	78
WHAT IS A FCL, AND HOW IS IT APPLIED?.....	79
HOW IS FCL PROCESSED WHEN A PARENT-SUBSIDIARY RELATIONSHIP EXISTS ON THE SIDE OF THE CONTRACTOR?.....	79
WHAT ARE THE RESPONSIBILITIES OF A CONTRACTOR UNDER A FCL?.....	79
WHAT IS A MFO AND HOW WOULD CLEARANCE WORK FOR MFO?	79
WHAT IF THE FCL COMES TO AN END?.....	79
WHAT IF SUBCONTRACTORS ARE INVOLVED?.....	79
WHO DETERMINES ELIGIBILITY OF ACCESS, AND WHO KEEPS THE RECORD?	80
WHAT KINDS OF INVESTIGATION MAY NEED TO TAKE PLACE?	80
WHAT GUIDELINES SHOULD A CONTRACTOR FOLLOW WHEN APPLYING FOR PCLS?	80
WHO ARE FOR SURE NOT ELIGIBLE FOR PCLS?.....	80
WHAT GUIDELINES SHOULD CLEARED PERSONNEL FOLLOW?	81
WHAT IS FOCI?.....	81
WHAT IS SPECIAL ABOUT FCL UNDER FOCI?	81
HOW ABOUT LIMITED FCL?.....	81
HOW ABOUT SSA?.....	81
WHAT ARE THE REQUIREMENTS WHEN FOCI COMES INTO PLAY?.....	81

WHAT ARE THE METHODS THAT MAY BE APPLIED TO NEGATE OR MITIGATE THE RISK OF FOREIGN OWNERSHIP OR CONTROL?	82
WHAT IS A GSC AND WHAT DOES IT DO?	82
WHAT IS TCP? WHO ESTABLISH IT AND HOW DOES IT WORK?.....	83
WHO PROVIDES THE NECESSARY TRAINING AND BRIEFING? IN WHAT MANNER?.....	83
WHAT SHOULD BE COVERED IN THE SECURITY BRIEFINGS?	83
WHAT IS SF312 AND HOW IS IT PROCESSED?.....	84
WHAT IS CLASSIFIED INFORMATION AND WHAT IS NOT?.....	84
WHAT IS AN ORIGINAL CLASSIFICATION AND WHAT ARE THE MARKING REQUIREMENTS?.....	84
HOW ARE DERIVATIVE CLASSIFICATION DECISIONS MADE?.....	84
WHO IS RESPONSIBLE FOR PROVIDING THE NECESSARY SECURITY CLASSIFICATION GUIDANCE?.....	85
WHAT SHOULD BE COVERED BY A CONTRACT SECURITY CLASSIFICATION SPECIFICATION? WHO SHOULD MAINTAIN IT?	85
WHAT SHOULD BE DONE UPON CONTRACT COMPLETION?	85
WHAT SHOULD BE DONE IF THE EXISTING CLASSIFICATION IS BELIEVED TO BE INACCURATE?	85
HOW SHOULD MARKING BE DONE IN GENERAL?	85
WHO IS RESPONSIBLE FOR THE MARKINGS?.....	86
HOW SHOULD MARKING BE DONE FOR COMPLEX DOCUMENTS?.....	86
HOW ABOUT PORTION MARKING?	86
WHAT OTHER MARKINGS MAY HAVE TO BE USED?.....	86
HOW ABOUT THE PROCESSING MATERIAL?.....	87
WHAT ARE THE SAFEGUARDING REQUIREMENTS FOR THE CONTRACTORS?.....	87
WHAT PROCEDURES AND POLICIES WOULD BE NECESSARY?.....	87
WHAT ABOUT ACCOUNTABILITY?.....	87
HOW ABOUT TRANSMISSION AND SHIPMENT?.....	88
HOW ABOUT STORAGE?	88

BCP, DRP AND RESPONSE MANAGEMENT.....89

RISK MANAGEMENT DEFINED	90
THE RISK MANAGEMENT STEPS	90
RISK MANAGEMENT AND THE IS PROFESSIONAL.....	91
RISK MANAGEMENT THE NIST WAY.....	91
BCP DEFINED.....	92
BCP vs BPCP vs COOP vs DRP	92
BCP PHASES.....	93
STAKEHOLDERS AND CRISIS COMMUNICATIONS	94
THE RISK ASSESSMENT FLOW.....	94
RISK VS THREAT AND VULNERABILITY	96
IDENTIFYING RISKS	96
LOSS CALCULATIONS.....	97
BUSINESS IMPACT ANALYSIS DEFINED	98
BIA GOALS AND STEPS	98
BIA CHECKLIST	99
PLANNING FOR CONTINGENCY.....	100

PREPARING FOR EMERGENCY RESPONSE	100
RESPONDING TO INCIDENTS AND MANAGING RECOVERY.....	101
TESTING THE PLAN.....	103
EXERCISING THE PLAN.....	104
VALIDATING THE PLAN	105
USER ACCEPTANCE.....	105
PLAN MAINTENANCE.....	106
PLAN SECURITY.....	106
BALANCED SCORECARD.....	107
BUSINESS PROCESS REENGINEERING	107
<u>COMPUTER FORENSICS.....</u>	108
THE PRIMARY GOAL.....	108
EVIDENCE COLLECTION AND SUBMISSION.....	109
DEFAMATION OF CHARACTER	110
TYPES OF EVIDENCE AND THE TOOL(S) TO USE	110
EXAMPLES OF COMMON INTERNET FRAUD SCHEMES.....	112
<u>CYCLE PLANNING.....</u>	113
<u>SDLC AND SECURITY INTEGRATION.....</u>	114
<u>INFORMATION SYSTEMS SECURITY ENGINEERING.....</u>	116
<u>REQUIREMENTS ANALYSIS.....</u>	118
<u>CRYPTOGRAPHY AND ENCRYPTION STANDARDS</u>	119
BROAD OVERVIEW	119
RSA	121
MD5 AND SHA	121
IPSEC, IKE AND SSL	122
ELLIPTIC CURVE	123
BLINDING	123
PADDING.....	123
OTP.....	123
DIGITAL CERTIFICATE	123
EES	124
OPENSSL.....	124
P3P.....	125
DISK BASED ENCRYPTION	126

<u>PHYSICAL AND ENVIRONMENTAL SECURITY.....</u>	<u>126</u>
A-B-C-D PLANNING.....	127
THE CONCEPT OF IPS.....	127
FACILITY DESIGN.....	128
FEMA RECOMMENDATION	128
DOOR MODIFICATIONS.....	129
UTILITY CONNECTIONS.....	129
ACCESSIBILITY AND SAFETY CONCERN	129
SPACE CONFIGURATION.....	130
DOOR DETAIL SCHEDULE	131
DESIGN THAT INVOLVES PROTECTING HIGH TECH EQUIPMENTS.....	131
DESIGN SPECIFICATION DOCUMENTS	131
PHYSICAL SECURITY SURVEY	132
PROTECTION IN DEPTH	133
PERIMETER DEFENSE	133
CCTV.....	134
CAMERA.....	134
MONITOR	135
RECORDER	135
SWITCH	135
OTHER GUIDELINES	135
ELECTRICAL LOCKS	136
CHAINLINK FENCING.....	137
CHAINLINK GATES	138
ELECTRONIC GATE OPENING	138
FENCE SIGNAGE.....	138
ENTRANCE SIGNAGE	138
FENCE MOUNTED SENSORS	138
EXTERIOR SENSORS	139
INFRARED SENSORS	139
MICROWAVE SENSORS.....	139
BISTATIC MICROWAVE SENSORS	139
DUAL TECHNOLOGY SENSORS.....	140
LINEAR BEAM SENSORS	140
OTHER PHYSICAL SECURITY CONCERNS	140
<u>CONTENT UPDATE.....</u>	<u>141</u>