

JOHNSON SPACE CENTER INFORMATION TECHNOLOGY SECURITY HANDBOOK

October 2001

Verify that this is the correct version for use.



**National Aeronautics and
Space Administration**

Lyndon B. Johnson Space Center
Houston Texas

JOHNSON SPACE CENTER
INFORMATION TECHNOLOGY SECURITY HANDBOOK

Approved By
JSC

Original signed by

Frank E. Martin, Ph.D.
Information Technology Security Manager

Original signed by

Jean E. Carter
Chief Information Officer

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
LYNDON B. JOHNSON SPACE CENTER
HOUSTON, TEXAS

October 2001

CHANGE LOG

Document Number: JPG 2810.1 **Title:** JSC I/T Security Handbook

Chg. # or Rev. letter	Date	Description	Pages Affected
	6/1998	Interim baseline release	All
	12/1999	New Version	All
	10/2000	Revised Section 5.11 and deleted section 5.12	
	10/2001	Added an index	
	10/2001	Changed the page numbering to be continuous rather restart for each section	Pages 1-317
	10/2001	Revised Section 2 to include cross-references to NPG 2810.1	Pages 7-14
	10/2001	Revised Section 3.1 to include Government Information Security Reform Act of 2000	Pages 16-18
	10/2001	Added Minimum Essential Infrastructure as a reason for designation as requiring special management attention in Section 5.11.1.4.	Page 61
	10/2001	Added NACB Virtual Private Network Policy in Section 6.5.8	Page 214
	10/2001	Added NACB External Email Policy in Section 6.5.9	Page 217
	10/2001	Clarify Penetration Test Authorization Requirements in Section 10.5.3	Page 256
	10/2001	Added reference to Government Information Security Reform Act of 2000 to Appendix E	Page 310

	10/2001	Updated Section 3.3.1.2 to show that the data base no longer tracks separate dates for the security controls review.	Page 20
	10/2001	Revised Section 10.1 Permissible Uses of Government I/T Systems to reflect current policy.	Page 246

CONTENTS

JPG 2810.1	I
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	I
ABBREVIATIONS.....	XIII

SECTION 1.....2

1.0	INTRODUCTION.....	3
1.1	APPLICABILITY AND SCOPE	3
1.2	COMPONENTS OF I/T SECURITY.....	3
1.3	GOALS AND OBJECTIVES OF THE JSC I/T SECURITY PROGRAM	4
1.4	ELEMENTS OF THE JSC I/T SECURITY PROGRAM.....	4
1.5	A RISK-BASED VERSUS A COMPLIANCE-BASED I/T SECURITY PROGRAM	5
1.6	THE ROLE OF REQUIREMENTS IN A RISK-BASED I/T SECURITY PROGRAM	6
1.7	APPLICABILITY OF ISO 9000 PROVISIONS	6
1.8	OVERVIEW OF JPG 2810.1	7
1.9	QUESTIONS AND COMMENTS.....	7

SECTION 2.....8

2.0	I/T SECURITY MANAGEMENT RESPONSIBILITIES	9
2.1	I/T SECURITY RESPONSIBILITIES BY POSITION.....	9
2.1.1	JSC Center Director	9
2.1.2	JSC Senior Staff.....	9
2.1.3	Chief Information Officer	9
2.1.4	Director, Human Resources	10
2.1.5	Director, Business Management.....	10
2.1.6	Director, Information Systems.....	11
2.1.7	Director, Center Operations.....	11
2.1.8	Information Technology Security Manager.....	11
2.1.9	Deputy Information Technology Security Manager	12
2.1.10	Line Manager.....	12
2.1.11	Organization Computer Security Manager.....	13
2.1.12	Alternate Organization Computer Security Manager (AOCSM)	14
2.1.13	JSC I/T Security Committee	14
2.1.14	System Security Administrator.....	14
2.1.15	JSC Network Access Control Board	14
2.2	I/T SECURITY SUPPORT FUNCTIONS.....	15

SECTION 3.....16

3.0	I/T SECURITY MANAGEMENT.....	17
3.1	THE LEGAL AND REGULATORY BASIS FOR I/T SECURITY	17
3.2	THE ELEMENTS OF THE JSC I/T SECURITY PROGRAM	19
3.3	I/T SECURITY MANAGEMENT AT THE CENTER LEVEL.....	20
3.3.1	Management Review, Evaluation, and Reporting	20
3.3.2	ITSM-Sponsored Analyses, Reviews, and Evaluations	24
3.3.3	The JSC I/T Security Engineering Team.....	25
3.4	OCSMS' ANNUAL REVIEW OF I/T SECURITY PROGRAM IN THE ORGANIZATION	26
3.5	REVIEWS BY INDIVIDUAL JSC ORGANIZATIONS	26
3.6	PERSONNEL SECURITY INVESTIGATIONS	26
3.7	I/T SECURITY AWARENESS AND TRAINING	27

3.8	CONFIGURATION MANAGEMENT OF THIS HANDBOOK	27
3.8.1	<i>Initiating a New Document or Initiating Changes to the Existing Document</i>	27
3.8.2	<i>Reviewing Requested Changes</i>	28
3.8.3	<i>Processing the Handbook and Proposed Changes to the Handbook</i>	28
3.8.4	<i>Releasing a New or Changed Handbook</i>	28
3.8.5	<i>Cancellation of this Handbook</i>	28

SECTION 4 29

4.0	INTRODUCTION TO I/T SYSTEM SECURITY ENGINEERING	30
4.1	OVERVIEW OF THE I/T SECURITY PLANNING PROCESS	31
4.2.1	<i>Determination of System Boundaries</i>	31
4.2.2	<i>Assignment as a Critical System or General Support System</i>	32
4.2.3	<i>Assignment of One or More Information Categories</i>	32
4.2.4	<i>Risk Analysis</i>	32
4.2.5	<i>Risk Reduction Analysis</i>	33
4.2.6	<i>Management Decision</i>	33
4.2.7	<i>Risk Reduction Actions</i>	33
4.2.8	<i>Life Cycle Implementation and Maintenance</i>	34
4.2.9	<i>Supporting Functions</i>	35
4.2.10	<i>Assignment of Responsibility, Security Plan, Periodic Review, and Authorization to Process</i>	35
4.3	REVIEW AND AUDIT OUTSIDE THE NORMAL CYCLE	36

SECTION 5 37

5.0	I/T SECURITY PLANNING	38
5.1	DETERMINING THE BOUNDARIES OF AN I/T SYSTEM	38
5.2	DETERMINING THE CATEGORY OF A JSC I/T SYSTEM	39
5.2.1	<i>Critical Systems</i>	39
5.2.2	<i>General Support Systems</i>	39
5.3	INFORMATION CATEGORIES	40
5.3.1	<i>Mission (MSN)</i>	41
5.3.2	<i>Business and Restricted Technology (BRT)</i>	41
5.3.3	<i>Scientific, Engineering, and Research (SER)</i>	42
5.3.4	<i>Administrative (ADM)</i>	42
5.3.5	<i>Public Access (PUB)</i>	42
5.4	RISK ANALYSIS	43
5.4.1	<i>Identify the Assets at Risk</i>	43
5.4.2	<i>Determine the Replacement Value of the Resources</i>	44
5.4.3	<i>Identify Threats to the Assets at Risk</i>	44
5.4.4	<i>Identify the Vulnerabilities</i>	45
5.4.5	<i>Vulnerabilities to Others</i>	47
5.4.6	<i>Determining and Prioritizing the Risks</i>	47
5.4.7	<i>Identification of Available Controls</i>	50
5.5	RISK REDUCTION ANALYSIS	51
5.5.1	<i>Identification of Potential Controls</i>	51
5.5.2	<i>Determination of Operational Feasibility of Recommended Controls</i>	52
5.5.3	<i>Recommendations to Management</i>	53
5.6	MANAGEMENT DECISION	53
5.7	RISK REDUCTION ACTIONS	54
5.8	LIFE CYCLE IMPLEMENTATION AND MAINTENANCE	55
5.9	ADDITIONAL REQUIREMENTS	57
5.9.1	<i>I/T Security Awareness and Training</i>	57
5.9.2	<i>Personnel Security Investigations</i>	57
5.9.3	<i>I/T Security Incidents</i>	57

5.10	COMPLETION OF I/T SECURITY METRICS.....	57
5.11	I/T SECURITY PLAN CONTENT.....	59
5.11.1	System Identification.....	60
5.11.2	Information Identification.....	63
5.11.3	Information Sharing.....	64
5.11.3	Risk Assessment and Analysis.....	64
5.11.5	Technical Controls.....	64
5.11.6	Public Access Controls.....	64
5.11.7	Rules of the System.....	65
5.11.8	Personnel Screening.....	65
5.11.9	Training.....	66
5.11.10	Contingency Planning.....	66
5.11.11	Incident Response.....	68
5.11.12	System Interconnection.....	68
5.11.13	Review of Security Controls.....	68
5.11.14	Authorization to Process.....	68

SECTION 6.....70

6.0	BASELINE I/T SECURITY REQUIREMENTS.....	71
6.1	TECHNICAL AND ADMINISTRATIVE SECURITY REQUIREMENTS.....	71
6.1.1	Mission Systems (MSN).....	72
6.1.2	Business and Restricted Technology (BRT).....	98
6.1.3	Scientific, Engineering, and Research (SER).....	122
6.1.4	Administrative (ADM).....	142
6.1.5	Public Access (PUB).....	162
6.2	NETWORK SECURITY REQUIREMENTS.....	180
6.2.1	Network Security Elements.....	181
6.2.2	Management Guidelines.....	182
6.2.3	Network Security Architecture Requirements.....	183
6.2.5	Network Host Requirements.....	184
6.3	PHYSICAL SECURITY REQUIREMENTS.....	199
6.3.2	Protection of I/T Resources from Fire and Water.....	201
6.3.3	Electric Power.....	201
6.3.4	Facility Housekeeping.....	201
6.3.5	I/T Resource Protection.....	202
6.4	I/T SECURITY PRACTICES DIRECTIVE.....	203
6.4.1	Risk Assessment TBD.....	203
6.4.2	Management and Operations TBD.....	203
6.4.3	Policies TBD.....	203
6.4.4	Requirements TBD.....	203
6.4.5	Information Management and Protection (B).....	205
6.4.6	Software Configuration Management.....	205
6.4.7	Network Requirements.....	206
6.4.8	Personnel Authentication (A).....	206
6.4.9	Training and Certification TBD.....	207
6.4.10	Auditing and Monitoring TBD.....	207
6.5	NACB POLICIES.....	207
6.5.2	Policy on Dial-in Access.....	208
6.5.3	Policy on Denying Network Access.....	208
6.5.4	Policy on Dedicated Lines.....	209
6.5.5	Policy on the Use of Standard Ports.....	211
6.5.6	Policy on File Transfer Protocol (FTP).....	211
6.5.7	Policy on the Distribution of Network Diagrams.....	212
6.5.8	Policy on the Use of Virtual Private Networks.....	213

6.6	WAIVER OF I/T SECURITY REQUIREMENTS	216
6.6.1	<i>Waiverable Versus Non-waiverable Requirements</i>	217
6.6.2	<i>Process for Submission of Waivers</i>	217

SECTION 7 220

7.0	I/T SECURITY AWARENESS AND TRAINING	221
7.1	THE BASIC TRAINING REQUIREMENT FOR ALL USERS	221
7.2	REQUIREMENTS AT AGENCY, CENTER, CONTRACTOR, ORGANIZATIONAL, AND SYSTEM LEVELS	222
7.2.1	<i>Agency-Level Training</i>	222
7.2.2	<i>Center-Level Training</i>	223
7.2.3	<i>Training Offered by Contractors</i>	224
7.2.4	<i>JSC Organization Level Training</i>	224
7.2.5	<i>System Specific Training</i>	224
7.3	TRAINING REQUIRED FOR PRIVILEGED USERS	224

SECTION 8 226

8.0	GRANTING ACCESS TO JSC'S I/T SYSTEMS	227
8.1	FEDERAL REQUIREMENTS	227
8.2	LINE MANAGEMENT'S RESPONSIBILITIES	228
8.3	REQUESTS FOR PERSONNEL SECURITY INVESTIGATIONS	229
8.4	MANAGEMENT GUIDELINES FOR GRANTING I/T ACCESS	230
8.4.1	<i>Granting Access to U. S. Citizens and Resident Aliens</i>	230
8.4.2	<i>Granting Access to Foreign Nationals Who Are Not International Partners</i>	231
8.4.3	<i>Granting Access to International Partners</i>	231
8.5	UNFAVORABLE INVESTIGATION RESULTS	232
8.6	LEVELS OF INVESTIGATION	232

SECTION 9 236

9.0	I/T SECURITY INCIDENT RECOGNITION, RESPONSE, AND REPORTING	237
9.1	I/T SECURITY INCIDENT DEFINED	237
9.2	HOW TO RECOGNIZE AN I/T SECURITY INCIDENT	238
9.3	HOW TO REPORT AN I/T SECURITY INCIDENT	238
9.3.1	<i>Reporting Computer Virus Infections</i>	239
9.3.2	<i>Reporting All Other I/T Security Incidents</i>	240
9.4	HANDLING INCIDENT INFORMATION	240
9.5	HANDLING EVIDENCE OF A COMPUTER CRIME	241
9.6	RETURNING EQUIPMENT TO SERVICE	241
9.7	REQUESTS FOR INFORMATION BY EXTERNAL AGENCIES	241

SECTION 10 244

10.0	GENERAL INFORMATION AND GUIDELINES	245
10.1	USE OF NASA INFORMATION TECHNOLOGY RESOURCES	245
10.1.1	<i>Questions and Answers about Use of Information Technology at JSC</i>	248
10.1.1	<i>Official Business Use of Government Resources</i>	250
10.1.2	<i>Ownership of Information in JSC-Owned I/T Systems</i>	251
10.1.3	<i>Monitoring Computer Systems Operated by or on Behalf of JSC</i>	252
10.1.4	<i>Privileges and Limitations of User Access</i>	252
10.1.5	<i>Extension of JSC Services to Remote Geographic Areas</i>	252
10.2	SOFTWARE USAGE	253

10.3	IMPORTED SOFTWARE INSPECTION FOR MALICIOUS CODE	253
10.4	NOTIFICATION TO USERS AT LOGON	253
10.5	JSC POLICY ON PENETRATION TESTING	254
10.5.1	<i>Penetration Testing Defined</i>	254
10.5.2	<i>The Need for Guidelines for Penetration Testing</i>	254
10.5.3	<i>Guidelines for Conducting Penetration Testing</i>	255
10.5.4	<i>Guidelines for Penetration Testing Conducted by the ITSM</i>	256
10.6	PRIVILEGED ACCESS OR ACCESS WITH LIMITED PRIVILEGES TO INFORMATION IN JSC'S I/T SYSTEMS	257
10.7	GUIDELINES FOR CONDUCTING COMPUTER SEARCHES	258

APPENDIX A 260

APPENDIX A JSC'S MAJOR INFORMATION SYSTEMS 261

INTEGRATED PLANNING SYSTEM (IPS)	261
SHUTTLE AVIONICS INTEGRATION LABORATORY (SAIL).....	262
SHUTTLE MISSION TRAINING FACILITY (SMTF).....	262
SPACE SHUTTLE SOFTWARE PRODUCTION FACILITY (SPF).....	262
SHUTTLE DRAWING SYSTEM (SDS).....	262
SHUTTLE TECHNICAL DOCUMENT MANAGEMENT SYSTEM (TDMS) 2	262
SHUTTLE MANAGEMENT PLANNING AND TRACKING SYSTEM	263
SHUTTLE PAYLOAD INTEGRATION LOADS VERIFICATION AND NASTRAN ANALYSIS SYSTEM	263
SPACE STATION VEHICLE MASTER DATA BASE (VMDB).....	263
INSTITUTIONAL NETWORK SERVICES (INS)	263
LIFE SCIENCES DATA SYSTEM (LSDS).....	263
BUDGET AND FINANCIAL ACCOUNTING SYSTEMS.....	264

APPENDIX B1 266

TECHNICAL THREATS.....267

EXTERNAL BREAK-INS	267
--------------------------	-----

ADMINISTRATIVE THREATS.....268

ACCESS DETERMINATION.....	268
---------------------------	-----

PHYSICAL THREATS 268

ACCESS CONTROL TO THE FACILITIES AND EQUIPMENT.....	268
VISITOR CONTROL	268

APPENDIX B2 270

APPENDIX B2 THREATS TO APPLICATIONS.....271

TECHNICAL THREATS.....271

EXTERNAL BREAK-IN TO THE I/T SYSTEM ON WHICH THE APPLICATION RUNS	271
---	-----

ADMINISTRATIVE THREATS.....272

ACCESS DETERMINATION.....	272
---------------------------	-----

PHYSICAL THREATS 272

ACCESS CONTROL TO I/T SYSTEM AND FACILITIES	272
EXTERIOR WINDOWS.....	273

APPENDIX B3 274

APPENDIX B3 THREATS TO NETWORKS.....275

APPENDIX C 278

APPENDIX C PRIORITIZED JSC I/T FUNCTIONS FOR EMERGENCY PREPAREDNESS PLANNING 279

PRIORITY 1	279
<i>Emergency Operations Center (EOC) - DA/Mission Operations</i>	279
<i>Flight Operations - DA/Mission Operations</i>	279
<i>Voice Communication - Bldg. 17 and 30 (Center Telecommunications System) - GA/Information Systems</i>	280
<i>Institutional Network Services (INS) - GA/Information Systems</i>	280
<i>Mission Evaluation Room (MER) Support - EA/Engineering</i>	280
<i>Medical Operations Support/MEDOPS - SA/Space & Life Sciences</i>	280
<i>Film/Video Analysis (Direct Mission Support) - SA/Space and Life Sciences</i>	281
<i>Other Voice Communication (CTS) - GA/Information Systems</i>	281
<i>Energy Management Control System (EMCS) - JA/Center Operations</i>	281
<i>Mission Support and Employee Communication - AP/Office of Public Affairs</i>	281
PRIORITY 2	282
<i>Flight Production - DA/Mission Operations</i>	282
<i>Space Shuttle Software Development - EA/Engineering</i>	282
<i>Mission Support-Shuttle Avionics Integration Laboratory (SAIL) - EA/Engineering</i>	282
<i>Shuttle Engineering Drawings—MA/Space Shuttle Operations and Integration Office</i>	283
<i>Shuttle Technical Documents Management—MA/Space Shuttle Operations and Integration Office</i>	283
<i>International Space Station Flight Software - OA/Space Station</i>	283
<i>Logistics Task Tracking/Inventory - JA/Center Operations</i>	283
<i>Procurement Operations (IPMS) - BA/Administration Directorate</i>	283
PRIORITY 3	283
<i>Process Personnel Actions - AH/Human Resources Office</i>	283
PRIORITY 4	284
<i>Institutional Class VI Computing - GA/Information Systems</i>	284
<i>Office Automation - DA/Mission Operations</i>	284
<i>Space Station Program Support - OA/Space Station</i>	284
PRIORITY 5	284
<i>Training/Simulation Software - CA/Flight Crew Operations</i>	284
<i>Space Shuttle Subsystem Management - EA/Engineering</i>	285
<i>Mission Support - Data Acquisition & Reduction - EA/Engineering</i>	285
<i>Mission Support - Engineering Analysis & Design - EA/Engineering</i>	285
<i>Mission Support - Simulation - EA/Engineering</i>	285
<i>PC Board CAD System - EA/Engineering</i>	285
<i>Task Tracking/Task Orders (Printing, Technical Services, Graphics) - GA/Information Systems</i>	285
<i>Institutional I/T Support - GA/Information Systems</i>	285
<i>Other Institutional Network Services - GA/Information Systems</i>	285
<i>Flight Evaluation Support - MA/Space Shuttle Operations and Integration Office</i>	286
<i>Extra Vehicular Activity (EVA) - SA/Space And Life Sciences</i>	286
PRIORITY 6	286
<i>AOD-LAN - CA/Flight Crew Operations</i>	286
<i>Level II Program Requirements Control Board (PRCB) Management - MA/Space Shuttle Program Office</i>	286
<i>Level II Requirements Baseline Maintenance - MA/Space Shuttle Program Office</i>	286

<i>Mission Integration and Program Scheduling - MA/Space Shuttle Operations and Integration Office</i>	286
<i>Payload Integration - MA/Space Shuttle Operations and Integration Office</i>	286
<i>Task Tracking/Task Order (Work Requests) - JA/Center Operations</i>	286
<i>Task Tracking/Inventory (Facility CAD/CAM) - JA/Center Operations</i>	286
PRIORITY 7	287
<i>Legal Systems/Docket Data Base - HA/Technology Transfer and Commercialization Office</i>	287
<i>Audit/Investigations - W-JS/Office of the Inspector General/JSC</i>	287
<i>Inspections and Assessments - W-JS/Office of the Inspector General/JSC</i>	287
<i>Operations/Aircraft Inventory Management - CA/Flight Crew Operations</i>	287
<i>General Operations Preparation - DA/Mission Operations</i>	287
<i>Design/Development/Integration - Data Acquisition & Reduction - EA/Engineering</i>	287
<i>Design/Development/Integration - Engineering Analysis & Design - EA/Engineering</i>	287
<i>Design/Development Integration - Subsystem Management - EA/Engineering</i>	287
<i>Design Development/Integration - Systems Engineering - EA/Engineering</i>	287
<i>Design/Development Integration - Systems/Payload Integration - EA/Engineering</i>	287
<i>Technology Tracking System (Tech Tracs) - HA/Technology Transfer and Commercialization Office</i>	287
<i>Central Security Control System (CSCS) - JA/Center Operations</i>	287
<i>NASA Internal Operations/PRACA - NA/SR&QA</i>	287
<i>Institutional VAX System - GA/Information Systems</i>	287
PRIORITY 8	288
<i>Workforce Reporting/Analysis - AH/Human Resources Office</i>	288
<i>Financial Management/Daily Operations - LA/Office of the Chief Financial Officer</i>	288
<i>Operations/Aircraft Maintenance - CA/Flight Crew Operations</i>	288
<i>Operations/Flight Records - CA/Flight Crew Operations</i>	288
<i>Operations/Aircraft Scheduling - CA/Flight Crew Operations</i>	288
<i>Training/Astronaut Training Scheduling - CA/Flight Crew Operations</i>	288
<i>Planning/Management - DA/Mission Operations</i>	288
<i>Finance/Contract - DA/Mission Operations</i>	288
<i>Design/Development/Integration - Basic & Applied Research - EA/Engineering</i>	288
<i>CLINLAB/Clinical Lab Support - SA/Space & Life Sciences</i>	288
<i>Anomaly Analysis ERSAF/SSEOPS - SA/Space & Life Sciences</i>	288
<i>Research - SA/Space & Life Sciences</i>	288
<i>Pre- and Post-Flight Data Analysis - MA/Space Shuttle Engineering Office</i>	288
PRIORITY 9	288
<i>Financial Management/Bi-Weekly Operations - LA/Office of the Chief Financial Officer</i>	288
<i>Human Resources - DA/Mission Operations</i>	288
<i>Administration & Management - EA/Engineering</i>	288
<i>Develop Software Technology - GA/Information Systems</i>	288
<i>Curatorial - SA/Space & Life Sciences</i>	288
<i>Security/Tracking (Security Management System) - JA/Center Operations</i>	288
<i>Task Tracking/Inventory (NEMS) - JA/Center Operations</i>	288
<i>Task Tracking/Images (Photo Data Base, Image Retrieval Data Base) - GA/Information Systems</i>	288
<i>Task Tracking System (NPDMS) - JA/Center Operations</i>	288
<i>General Office Automation - All JSC Organizations</i>	288
PRIORITY 10	289
<i>Support Award Programs (Client Server) - AH/Human Resources Office</i>	289
<i>Process Astronaut Applications (Client Server) - AH/Human Resources Office</i>	289
<i>Miscellaneous Functions - AH/Human Resources Office</i>	289
<i>O/T Management System - AH/Human Resources Office</i>	289
<i>Employee Benefit Support - AH/Human Resources Office</i>	289
<i>Financial Management/End-of-month Operations - LA/Office of the Chief Financial Officer</i>	289
<i>Facilities - DA/Mission Operations</i>	289
<i>Task Tracking/Correspondence Management - GA/Information Systems</i>	289
<i>Public Services/Tours - AP/Office of Public Affairs</i>	289
<i>Task Tracking/Library Support - GA/Information Systems</i>	289

APPENDIX D	290
APPENDIX D	291
<i>GLOSSARY</i>	291
RESIDUAL RISK	304
APPENDIX E	308
APPENDIX E	309
APPENDIX F	310
BIBLIOGRAPHY	310
INDEX	312

Figures

FIGURE	PAGE
5-1 RISK VALUE COMPUTATION	52
6-1 VPN TEST MATRIX	220

Tables

TABLE PAGE

8-1 GRANTING ACCESS TO U.S. CITIZENS AND RESIDENT ALIENS 8-7

**8-2 GRANTING ACCESS TO FOREIGN NATIONALS WHO ARE NOT INTERNATIONAL PARTNERS
8-8**

8-3 GRANTING ACCESS TO INTERNATIONAL PARTNERS 8-9

Abbreviations

ADP	automated data processing
ADM	Administrative
AMPTS	Automated Mission and Payload Tracking System
AOCSM	Alternate Organization Computer Security Manager
ASRB	Annual Security Refresher Briefing
BARS	Baseline Accounting Reporting System
BAS	Basic Accounting System
BFS	Backup Flight Software
BRT	Business and Restricted Technology
CAD	computer-aided design
CAM	computer-aided manufacturing
CC	cluster controller
CCAS	Contractor Cost Accrual System
CCC	Control Center Complex
ITSM	Information Technology Security Manager
CENBUD	Central Budget System
CIO	Chief Information Officer
CIS	Center Information System
COD	Center Operations Directorate
COTS	commercial off-the-shelf
CPEOC	Community Partners Emergency Operations Center
CS	Critical System
CSCS	Central Security Control System
CTS	Center Telecommunications System
DITSM	Deputy Information Technology Security Manager
DDT&E	Design, Development, Test and Evaluation
DES	Data Encryption Standard
DNS	Domain Name Servers
ECF	Engineering Computer Facility

EMCS	Energy Management Control System
EOC	Emergency Operations Center
ERT	Emergency Response Team
EVA	Extra Vehicular Activity
FDCF	Flight Design Computational Facility
FEP	front-end processor
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FPS	Flight Planning System
FSO	Facility Security Officer
GSS	General Support System
HNAC	NASA Headquarters National Agency Check
HQS	NASA Headquarters
IBAS	Interactive Basic Accounting System
ICFAS	Interactive Consolidated Fiscal Accounting System
ID	identifier
IMIC	Integrated Management Information Center
INS	Institutional Network Services
IP	International Partners
IPMS	Integrated Procurement Management System
IPS	Integrated Planning System
ISAC	Information Systems Analysis & Integration Systems Contract
ISO	International Organization for Standardization
I/T	Information Technology
ITAR	International Traffic In Arms Regulations
ITSM	Information Technology Security Manager
JCAR	JSC Corrective Action Request
JOCS	Job Order Cost System
JPG	JSC Policy Guidelines
JSC	Johnson Space Center
LAN	local area network

LIM	limited-function
LSDS	Life Sciences Data System
LSFEP	Life Sciences Flight Experiments Program
MBF	Mission Build Facility
MCC	Mission Control Center
MEDICS	Medical Information Computer Systems
MEDOPS	Medical Operations Support
MER	Mission Evaluation Room
MIN	minimum requirements
MOD	Mission Operations Directorate
MSFC	Marshall Space Flight Center
MSN	mission
MRCS	Mission Requirements Control System
NA	network analyzer
NACC	NASA Automated Data Processing Consolidated Center
NASA	National Aeronautics and Space Administration
NASIRC	NASA Automated Systems Incident Response Capability
NEMS	NASA Equipment Management System
NPD	NASA Policy Directive
NPG	NASA Policy Guideline
NPPS	NASA Personnel and Payroll System
OIG	NASA Office of Inspector General
OMB	Office of Management and Budget
OCSM	Organization Computer Security Manager
PAO	Public Affairs Office
PASS	Primary Avionics Software System
PC	personal computer
PCASS	Program Compliance Assurance and Status System
PL	Public Law
POIC	Payload Operations Integration Center
POP	Program Operating Plan

PRACA	Problem Reporting and Corrective Action
PRCB	Program Requirements Control Board
PUB	Public Access
RFP	request for proposal
RIF	Reduction in Force
SAIL	Shuttle Avionics Integration Laboratory
SC	security critical
SDF	Software Development Facility
SDIL	Software Development Integration Laboratory
SDS	Shuttle Drawing System
SER	Scientific, Engineering, and Research
SLP	System Level Procedure
SMTF	Shuttle Mission Training Facility
SOW	statement of work
SPF	Software Production Facility
SSVTF	International Space Station Verification and Training Facility
STIC	Scientific and Technical Information Center
STRCS	Space Transportation Reimbursable Cost System
SUBAUTH	Sub-Authorization System
TCMS	Test, Checkout, and Monitoring System
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMS2	Shuttle Technical Document Management System
UNLIM	unlimited-function
VMDB	Vehicle Master Data Base
VRT	Virus Response Team

SECTION 1

INTRODUCTION

1.0 INTRODUCTION

An I/T security program only exists because it helps to protect valuable information from exploitation. This handbook's purpose is to document the Johnson Space Center (JSC) Information Technology Security Program and to provide readers with the knowledge necessary to protect their sensitive information from theft, destruction, or loss. This handbook implements the National Aeronautics and Space Administration (NASA) Information Technology Security Program, documented in NASA Policy Guideline (NPG) 2810.1, at JSC and serves as a single-volume reference for JSC's processes and guidelines.

1.1 APPLICABILITY AND SCOPE

This document applies to all civil servants and contractor employees at JSC sites. Individuals doing work at a college, university, or research establishment under a contract or grant from JSC are included in the JSC I/T Security Program to the extent prescribed by their contract. However, when persons covered by such an arrangement have access to JSC information technology resources, they still must still abide by the provisions of this handbook.

This document rescinds and replaces in its entirety JSCM 2410.11, the *Johnson Space Center Automated Information Systems Security Manual*, October 1992.

This handbook applies only to the security of unclassified automated information, applications, and computer and telecommunications systems. The processing of classified automated information and secure telecommunications is the responsibility of the JSC Security Branch. The requirements for classified processing may be found in the current edition of JSC Policy Guideline (JPG) 1600.3A, the *JSC Security Procedures and Guidelines*, (ref. 5) or by contacting the JSC Security Branch.

1.2 COMPONENTS OF I/T SECURITY

Information technology security has three components:

- a. **Integrity**, the ability to ensure that sensitive automated information, the applications that process the data, the information technology systems that run the software, and the hardware configuration, connectivity and the status of privilege settings cannot be altered during storage or transmission;
- b. **Availability**, the ability to ensure that sensitive data, applications, and systems are there to be accessed when and where needed; and,
- c. **Confidentiality**, the ability to ensure that information is disclosed only to those who have a valid business needs to possess it.

Although each I/T security problem is unique, all of them may be solved by taking the proper mix of technical and managerial controls that gives the appropriate weight to each of the three components above.

1.3 GOALS AND OBJECTIVES OF THE JSC I/T SECURITY PROGRAM

The goal of the JSC I/T Security Program is to ensure that appropriate, cost-effective levels of integrity, availability, and confidentiality are applied to the protection of all of JSC's sensitive information and systems in support of the Center's missions, programs, and functions. To accomplish this goal, the Chief Information Officer (CIO) has established the following objectives for the JSC I/T Security Program and appointed the Information Technology Security Manager (ITSM) overall policy and compliance responsibility:

- a. To assure that all I/T systems in the JSC community have a plan for achieving and maintaining an appropriate, cost-effective level of security which is based on a proactive life-cycle, risk-based approach to I/T security, including planning for contingency operations
- b. To assure that all individuals who can bypass system security controls and processes are identified in accordance with the sensitivity of information or type of access they require such that an appropriate personnel security investigation may be accomplished
- c. To assure that all personnel in the JSC community, both civil service and contractor, understand their individual responsibilities through an appropriate I/T security awareness and training program
- d. To assure that effective incident response and reporting processes exist and that all personnel know how to use them
- e. To assure that appropriate metrics are collected and reported in order to permit management to gauge the effectiveness of the program

1.4 ELEMENTS OF THE JSC I/T SECURITY PROGRAM

On October 30, 2000 the President signed into law the FY2001 Defense Authorization Act (Public Law 106-398) including Title X, subtitle G, "Government Information Security Reform (The Security Act). The Security Act amends the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. Chapter 35) by enacting a new subchapter on "Information Security" which primarily addresses the program management and evaluation aspects of security. For unclassified information technology systems, the Office of Management and Budget (OMB) retains its existing policy authority under the PRA and the Clinger-Cohen Act of 1996. Except for new annual program reviews, the role of the agency Inspector General, and the annual reporting requirement, the Security Act essentially codifies the 1996 requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." The Security Act also requires agencies to incorporate

security into the life cycle of agency information systems. . This edition of JPG 2810.1 has been brought up to date and reflects the newest Federal and Agency guidance in effect on the date of publication.

NASA as an Agency has not changed in its reliance upon a risk-based approach to I/T security. Selection of security controls based on risk remains central to the methodology, but the process and documentation have been simplified. The JSC I/T Security Program has the following elements:

- a. Each I/T system has a knowledgeable individual assigned responsibility for the security of that system.
- b. The security processes and controls will be documented for every system in an I/T security plan.
- c. A periodic review of security controls of each I/T system will be conducted at least every three years or upon significant change, whichever occurs first.
- d. An appropriate JSC management official has given authority for each I/T system to process based on implementation of its security plan.
- e. All individuals who access information in an I/T system operated by or on behalf of the Federal Government will be trained commensurate with their responsibilities.
- f. JSC managers have appropriate guidelines to grant access to their systems, including requiring personnel security investigations when individuals can bypass I/T security controls and processes.
- g. I/T security incident recognition, response, and reporting processes are in place for every I/T system.

The remainder of this handbook will show how these program elements will be integrated into a comprehensive I/T security program

1.5 A RISK-BASED VERSUS A COMPLIANCE-BASED I/T SECURITY PROGRAM

Generally speaking, two philosophies have historically governed computer security programs, compliance-based and risk-based. The compliance-based approach is highly structured and depends upon a set of rules issued by a high enough Government or corporate authority that the rules can be made mandatory for all participants in the program. Compliance-based programs provide a common set of security goals for the participants but leave the least flexibility to the individual system managers who are accountable for the successful operation of the system. A risk-based security program, on the other hand, places the burden directly upon line managers to discern and understand their risks and then make reasonable decisions about what risks to accept versus what risks to mitigate or correct. NASA

and JSC have implemented a risk-based program, provided that certain minimum baseline criteria are met.

Experience has shown that the cost-effectiveness and flexibility that result from a risk-based approach far outweigh any of its potential disadvantages. It is not the intention of the program to eliminate all risk; rather, the intent is to provide and implement a sound, logical methodology that is consistent with good systems engineering practice by which risks can be understood, assessed, and managed. I/T security, then, is not a separate endeavor; it is a process that is integrated into a system's entire life cycle.

1.6 THE ROLE OF REQUIREMENTS IN A RISK-BASED I/T SECURITY PROGRAM

The minimum baseline I/T Security requirements are described in Appendix A of NPG 2810.1 and section 6 of this document. To provide the proper level of I/T security in their systems, managers should:

- a. Perform a risk analysis to determine and prioritize their risks
- b. Impose security controls as described in NPG 2810.1, Appendix A and section 6 of this document (or develop equivalent solutions if necessary, depending upon their particular system architecture), to mitigate or correct the risks determined in the risk analysis; and
- c. Impose more stringent technical or managerial controls if the risk analysis shows that the recommended baseline controls of NPG 2810.1, Appendix A and section 6 of this document are insufficient

There are several reasons why managers should be scrupulous in imposing at least the minimum security controls that section 6 requires. First, in JSC's increasingly interconnected community, a weakness in one area represents a risk to everyone else that shares common resources. Second, by implementing where possible at least the minimum baseline set of controls, the manager assures the Agency and the public that the information entrusted to that manager's care is protected to a known standard. Third, ignoring a proper baseline set of security controls and then being forced to recover from an external intruder's attack has more than once led to excessive cost.

1.7 APPLICABILITY OF ISO 9000 PROVISIONS

The JSC I/T Security Program is designed not only to fulfill the applicable Federal and Agency directives regarding I/T security but also to meet the provisions of the JSC Quality Program. This handbook is a quality document under JSC's Quality Program. The current edition is available through the JSC Quality Management System (QMS) Electronic Document Repository. Readers should first check this repository for the current edition any time they use this handbook.

1.8 OVERVIEW OF JPG 2810.1

This handbook is divided into sections that generally follow the elements of the JSC I/T Security Program.

- a. **I/T Security Management Responsibilities, section 2**, describes the duties of line management, computer security managers, support personnel, end users, and others who have duties in the JSC I/T Security Program.
- b. **I/T Security Management, section 3**, identifies and describes the management processes and metrics integral to the program.
- c. **Introduction to I/T System Security Engineering, section 4**, provides an end-to-end overview of the role of the I/T security planning process.
- d. **I/T Security Planning, section 5**, provides the detailed instructions and examples for completing a risk analysis and then using this risk analysis to prepare the appropriate security planning documents.
- e. **Baseline I/T Security Requirements, section 6**, establishes technical, administrative, and physical requirements that provide a minimum baseline for the JSC's I/T systems.
- f. **I/T Security Awareness and Training, section 7**, establishes the requirements for initial and continuation training and describes what training classes and materials are available to the JSC community from the ITSM.
- g. **Granting Access to JSC's I/T Systems, section 8**, provides guidelines and administrative requirements for the personnel screening and risk management processes that meet the intent of Federal law, Office of Personnel Management, and NASA regulations and is sufficient to protect sensitive I/T resources.
- h. **I/T Security Incident Recognition, Response, and Reporting, section 9**, provides guidelines and administrative requirements for recognizing, responding to, and reporting I/T security incidents.
- i. **General Information and Guidelines, section 10**, provides guidance on various matters of ethics, regulation, and policy that are of concern to JSC's computer users.

1.9 QUESTIONS AND COMMENTS

The CIO delegates to the Information Technology Security Manager responsibility for the JSC Information Technology Security Policy and for the content of this handbook. Readers' questions are invited at any time.

This handbook follows a configuration management process described in section 3.7. Readers who wish to submit changes to this handbook may submit them at any time in accordance with this process.

SECTION 2

I/T SECURITY MANAGEMENT RESPONSIBILITIES

2.0 I/T SECURITY MANAGEMENT RESPONSIBILITIES

All JSC and contractor personnel who manage, use, program, or operate JSC I/T or telecommunications resources have responsibilities for ensuring that appropriate levels of integrity, availability, and confidentiality are maintained throughout the life cycles of these systems. The purpose of this section is to define these responsibilities by position.

2.1 I/T SECURITY RESPONSIBILITIES BY POSITION

2.1.1 JSC Center Director

The responsibilities of the Center Director with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.1. The Center Director has overall responsibility for the JSC I/T Security Program. The Director will ensure that the following tasks are accomplished:

- a. Developing, implementing, documenting, and monitoring the JSC I/T Security Program.
- b. Incorporating NASA, other Government Agency, or foreign national I/T security processing needs, in accordance with agreements among agencies.
- c. Appointing a Chief Information Officer (CIO) to whom responsibility for the JSC I/T Security Program has been delegated.
- d. Ensuring that appropriate I/T security requirements are included in all contracts and statements of work (SOWs) for acquisition, operation, or disposal of critical system (CS) and general support system (GSS) (where these terms are as defined in section 5.3) equipment, applications, and related services.

2.1.2 JSC Senior Staff

The responsibilities of the JSC Senior Staff with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.3. The JSC Senior Staff members have responsibility for the following:

- a. Implementing the JSC I/T Security Program in their respective organizations.
- b. Appointing a civil servant to serve as the Organization Computer Security Manager (OCSM) for that organization.
- c. At the Senior Staff member's option, appointing a second civil servant to serve as alternate OCSM.

2.1.3 Chief Information Officer

The responsibilities of the Chief Information Officer (CIO) with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.2. The

Center Director has delegated the responsibility for the JSC I/T Security Program to the CIO. The CIO has the following I/T security duties:

- a. Establishing and maintaining the JSC I/T Security Program ensures the safety of I/T investments within scope of the JSC I/T Program as well as compliance with federal and NASA I/T Security requirements.
- b. Reviewing and approving all network interfaces between JSC and other NASA facilities, contractor facilities, and all external communications.
- c. Reviewing and approving significant connectivity between organizations within JSC where critical systems are involved.
- d. Appointing the Information Technology Security Manager (ITSM).
- e. Working in conjunction with other organizations to ensure that sufficient resources are available to the ITSM to implement and maintain the JSC I/T Security Program.
- f. Approving the JSC I/T Security Handbook, JPG 2810.1.
- g. Approving searches of computers when probable cause of misuse exists.

2.1.4 Director, Human Resources

The responsibilities of the Human Resources Director with respect to Information Technology Security are described in NPG 2810.1, Section 2.3.2. The Director, Human Resources, is responsible for the following:

- a. Coordinating with the ITSM to develop a Center I/T Security Training Awareness and Training Plan to ensure that the Center's user community has the awareness, knowledge, and skills necessary to protect NASA information, data, and systems
- b. Developing an I/T Security Awareness and Training Plan
- c. Identifying requirements for I/T Security Awareness and Training
- d. Identifying sources for providing the training
- e. Budgeting funds for both initial and follow-on I/T security curricula
- f. Maintaining records that show who has received I/T security training

2.1.5 Director, Business Management

The responsibilities of the Director of Business Management with respect to Information Technology Security are described in NPG 2810.1, Section 2.3.4. The Director of Business Management is responsible for developing and implementing policies and procedures to incorporate JPG 2810.1 requirements into all JSC contracts.

2.1.6 Director, Information Systems

The responsibilities of the Director of Information Systems with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.9. The Director, Information Systems, is responsible for the following:

- a. Providing essential staff support for the JSC I/T Security Program.
- b. Maintaining appropriate security for JSC's Center-level telecommunications networks.

2.1.7 Director, Center Operations

The responsibilities of the Director of Center Operations with respect to Information Technology Security are described in NPG 2810.1, Section 2.3.1. The Director, Center Operations, is responsible for providing the resources to conduct personnel security investigations as prescribed by NPG 2810.1, Section 4.5 and JPG 2810.1, Section 8.

2.1.8 Information Technology Security Manager

The responsibilities of the Information Technology Security Manager with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.4. The ITSM is appointed by the CIO and is delegated day-to-day management responsibility for the JSC I/T Security Program. The ITSM has the responsibility for the following:

- a. Establishing the overall direction and structure of the JSC I/T Security Program, implementing Federal and Agency I/T security policy, and developing requirements and guidelines.
- b. Developing and maintaining the current edition of the JSC I/T Security Handbook, JPG 2810.1.
- c. Preparing the annual JSC I/T Security Program Plan.
- d. Establishing a management process that assures that the security risks inherent in I/T systems, applications, and facilities are identified and evaluated and that appropriate actions are taken by line managers to reduce risks to an acceptable level.
- e. Conducting periodic analyses, reviews, and evaluations of I/T Security Program implementation.
- f. Chairing the JSC I/T Security Committee.
- g. Reviewing and recommending concurrence with CS and GSS SMA designations as determined by the respective JSC line managers. Notwithstanding any other assigned responsibilities in this document, the final authority for I/T security rests with the CIO.

- h. Providing status to NASA Headquarters (HQS), the Principle Center for I/T Security, and the Center Director.
- i. Serving as the point of contact for information on I/T security incidents with organizations external to JSC.
- j. Serving as the interface for I/T security matters with all organizations external to JSC.
- k. Assuring that processes are in place that require all individuals in the JSC community who access I/T systems operated by or on behalf of the U. S. Government receive appropriate I/T security awareness and training.
- l. Assuring that all JSC OCSMs and alternate OCSMs receive appropriate training.

2.1.9 Deputy Information Technology Security Manager

There is no description of responsibilities for deputy ITSM in NPG 2810.1. The DITSM has responsibility for the following:

- a. Serving as the JSC ITSM in the ITSM's absence.
- b. Supporting the development of requirements and guidelines for the JSC I/T Security Program.
- c. Supporting the development and maintenance of the current edition of the JSC I/T Security Handbook, JPG 2810.1.
- d. Supporting the development of the annual JSC I/T Security Plan.
- e. Maintaining the JSC I/T Security Data Base as prescribed in section 3.3.1.2.
- f. Preparing status reports on the JSC I/T Security Program as required.
- g. Assuring that effective procedures exist and are followed to provide adequate I/T Security Incident Response as described in NPG 2810.1, Section 2.3.3 and JPG 2810.1 Section 9.

2.1.10 Line Manager

The responsibilities of the line manager with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.7. All JSC's I/T systems are assigned to JSC civil service line managers who will be responsible for their security. This is true for all systems regardless of whether they are designated as Critical Systems or General Support Systems. If a system is operated and managed by contractors, these contractors report via a civil service contracting officer to a civil service line manager. Typically, a line manager is at the branch or division level. The line manager with primary responsibility for the security of a system is responsible for the following:

- a. Ensuring that adequate and appropriate I/T security controls are defined, implemented, and tested consistent with the line manager's determination of acceptable levels of risk.
- b. Ensuring that the security risks of the system under the line manager's cognizance are identified and evaluated and that adequate safeguards are implemented consistent with the line manager's determination of acceptable risk levels.
- c. Certifying the adequacy and appropriateness of security controls before the initial operation of a new system and periodically throughout the life cycle.
- d. Developing and implementing a system security plan and periodically testing the contingency operations that the plan prescribes.
- e. Appointing and properly training a system security administrator to act as the focal point for that system or application.
- f. Reporting suspected I/T security incidents to the OCSM and to line management.

2.1.11 Organization Computer Security Manager

The responsibilities of the organization computer security manager with respect to Information Technology Security are described in NPG 2810.1, Section 2.2.6. The OCSM is responsible for that organization's I/T security program. The OCSM serves as the critical communication link to and from that organization for all I/T security matters and has the following responsibilities:

- a. Establishing a management control and communications process to ensure that the organization's I/T security program is implemented consistent with the current edition of JPG 2810.1.
- b. Serving as the organization's representative to the JSC I/T Security Committee, representing the organization's director or office chief on all I/T security matters, and casting that organization's vote on matters of I/T security policy. Note that this policy-making role of the OCSM necessitates that all OCSMs and alternate OCSMs be civil servants.
- c. Reporting suspected I/T security incidents to the ITSM and the organization's director or office chief.
- d. Reporting periodically to the ITSM and the organization's director or office chief on the status of I/T security planning in that organization, including acting as the sole authorized source for that organization's inputs to the JSC I/T Security Data Base.
- e. Reviewing annually the IT Security Plans for the organization's systems.

- f. Submitting electronic and printed copies of each I/T Security Plans to the ITSM. If the contingency plan is set out in a separate document, that document must also be submitted to the ITSM since it is an integral part of the security plan.
- g. Serving as the organization's representative to the Network Access Control Board unless the organization has named another individual to be the representative.

2.1.12 Alternate Organization Computer Security Manager (AOCSM)

The AOCSM fulfill security responsibilities in the absence of the OCSM. In addition, the AOCSM participates in all activities of the JSC I/T Security Committee.

2.1.13 JSC I/T Security Committee

The JSC I/T Security Committee is chaired by the ITSM with the DITSM as vice chair. The committee consists of the OCSMs, AOCSMs and individuals who have designated as contractor I/T Security Points of Contact. Contractor I/T Security Points of Contact have voice but no vote. The JSC I/T Security Committee is the senior advisory body to the ITSM on all matters of I/T security policy and practice at JSC. The members report to the ITSM any significant developments affecting the security status of their organization's I/T systems.

2.1.14 System Security Administrator

Although JSC line managers are responsible for the security of their critical systems and applications, they may assign the day-to-day security activities to a system security administrator who may be either a civil servant or a contractor. In this case, the duties of the position are as each line manager prescribes. Typical responsibilities for a critical system security administrator include the following:

- a. Reviewing security requirements and specifications for new or significantly modified systems.
- b. Developing and conducting systems tests that demonstrate the existence and effectiveness of specified security features.
- c. Conducting a risk analysis and preparing the system security plan.
- d. Managing day-to-day operational security activities.
- e. Reporting all suspected incidents in accordance with section 9.

2.1.15 JSC Network Access Control Board

A representative from the CIO office chairs the JSC Network Access Control Board (NACB). The NACB is comprised of "Standing," "Ad hoc," and Ex-officio members. Standing members are permanently assigned to the Board and will participate in all Board decisions. The Mission of the NACB is to assure, through the appropriate

review and concurrence processes, a level of risk relative to security and integrity of JSC networked resources which meets or exceeds Agency and Center requirements and expectations while maintaining an I/T environment which fully supports the Agency and Center missions.

2.2 I/T SECURITY SUPPORT FUNCTIONS

I/T security support functions include other tasks that may be required, depending upon the size, complexity, or criticality of the system or application. Support functions may include auditor, user ID administrator, password administrator, tape librarian, or any other duty needed to support the operations of that particular system or application. The responsible line manager determines the nature and scope of these positions and assigns the duties as required.

SECTION 3

I/T SECURITY MANAGEMENT

3.0 I/T SECURITY MANAGEMENT

Whereas section 2 described the responsibilities of the people who have a role in the JSC I/T Security Program, section 3 discusses the elements of the program itself and how it is implemented, what kinds of information are kept in the JSC I/T Security Data Base, what kinds of analyses, reviews, and evaluations may be performed, and generally establishes the management tools by which the JSC I/T Security Program is conducted. This section will also describe the elements by which the program is assessed and will tie these program elements back to their governing Federal directives. From this section the reader will gain an understanding of why any given task in I/T security is necessary. All tasks in I/T security trace back to good business practices, to requirements imposed by Federal directive, or, occasionally, to a need to enforce the law.

3.1 THE LEGAL AND REGULATORY BASIS FOR I/T SECURITY

Information entrusted to JSC is valuable and the protection of its integrity, availability, and, in some cases, confidentiality is a matter of good business ethics and public trust. For some kinds of information, protection is mandated by law. Therefore, all users of I/T systems and the managers who oversee them must be diligent in ensuring that information under their control is appropriately protected.

While the ethical responsibility is a serious one, all Federal Agencies also have a charter founded in law to conduct I/T security programs. The requirement to conduct I/T security programs is articulated clearly in Public Law (PL) 100-235, *The Computer Security Act of 1987* (ref. 2). This statute establishes a Federal mandate that sensitive information in a computer operated by or on behalf of the United States Government will be protected.

The Computer Security Act of 1987 did not concern itself with the means of implementation; that task is assigned to the Office of Management and Budget of the Executive Office of the President. OMB has carried out that task in Appendix III of OMB Circular A-130, *Management of Federal Information Resources* (ref. 1). A copy of OMB Circular A - 130 can be found on the JSC CIO web page. It is from this document that NASA has derived the basic elements that make up the Agency's I/T Security Program. The elements are the same for all Federal Agencies; NASA has interpreted them so that they make sense in a NASA context. JSC, in turn, has taken the Agency-level elements and adapted them to the needs of the JSC community.

Public Law 100-235, *The Computer Security Act of 1987*, began a major overhaul of the way Federal Agencies conduct I/T security activities. By February 1996, new instructions for implementing the Computer Security Act had been issued via a completely-revised version of Appendix III to OMB Circular A-130. Section 5 of this handbook implements the I/T security planning requirements of Appendix III.

On October 30, 2000 the President signed into law the FY2001 Defense Authorization Act (Public Law 106-398) including Title X, subtitle G, “Government Information Security Reform (The Security Act). The Security Act amends the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. Chapter 35) by enacting a new subchapter on “Information Security” which primarily addresses the program management and evaluation aspects of security. For unclassified information technology systems, the Office of Management and Budget (OMB) retains its existing policy authority under the PRA and the Clinger-Cohen Act of 1996. Except for new annual program reviews, the role of the agency Inspector General, and the annual reporting requirement, the Security Act essentially codifies the 1996 requirements of OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources.” The Security Act also requires agencies to incorporate security into the life cycle of agency information systems.

Those readers who are responsible for security planning for JSC’s I/T systems are encouraged to become familiar with the documents mentioned above; they are fundamental to the methodologies described in this section. When reading OMB Circular A-130, readers should bear in mind some important points that will significantly aid their understanding of NASA’s and JSC’s approach.

First, readers should remember that OMB Circular A-130 applies to all Federal Agencies. Because it constitutes the governing Federal directive that creates the I/T Security Program within the Federal Government, implementing the provisions of the circular is neither optional nor waivable.

Second, Federal Agencies use I/T systems in a bewildering variety of tasks, from air traffic control to printing benefit checks to collecting taxes to maintaining libraries and patent records to conducting space flight. Writing one policy statement that can be easily applied in all circumstances and still remain flexible enough to accommodate the continuing infusion of new technology is a daunting task. OMB selected a paradigm that would fit most of the Federal Agencies most of the time.

OMB selected a paradigm that categorized all Federal I/T processing under two areas: general support systems and major applications. However, the word *application* as OMB uses it has a very different meaning from the meaning that the computer industry normally associates with the term. OMB defines *application* to be a “use of information resources (information and information technology) to satisfy a specific set of user requirements.” A *major application*, then, is “an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.” In general, then, *major applications* are considered to be the most important functions that the Agency must perform to accomplish its mission, essentially the lifeblood of the Agency.

In order that the reader not be left in confusion, JSC has explicitly defined its major applications. The definitions will be found in section 5.2. In this handbook, the

concept that OMB refers to as a **major application**, JSC will call a **critical system**.

OMB's paradigm intended that major applications would run on general support systems. General support systems were intended to provide computational power; major applications were the functions that got the Agency's job done. NASA readers of this handbook will quickly realize that information technology as it is used in NASA today generally does not follow this paradigm. Only in legacy systems, such as some of the few remaining mainframe operations, does this paradigm hold. However, OMB left the definition of the term *application* broad enough so that it may include hardware, software, networks, and even facilities where it is reasonable to do so. This permits I/T systems to be bounded in reasonable ways for the purposes of security planning. Therefore, the NASA Personnel and Payroll System, a collection of software packages (an "application" in the traditional sense) is a major application, but so is the Mission Control Center.

The definition of *general support system* is much simpler. For NASA's purposes, all other I/T systems or applications that remain after the major applications have been defined are general support systems.

The latest version of Appendix III (January 1996) also resolved another important issue regarding information sensitivity. All information in an I/T system operated by or on behalf of the Federal Government is considered sensitive to some degree and must have an appropriate level of protection. Appendix III did not attempt to prescribe the protective measures but left determining specific controls to the results of a risk analysis. Nevertheless, Federal Agencies no longer have the option to designate some information as non-sensitive and exempt from I/T security considerations.

3.2 THE ELEMENTS OF THE JSC I/T SECURITY PROGRAM

This section describes the elements of the JSC I/T Security Program.

- a. Assignment of Security Responsibility: Every CS and GSS will have security responsibility assigned to an individual knowledgeable in the nature of the information processed and who is competent to apply and manage appropriate security controls. The reader will find guidance in section 5 for applying this element.
- b. I/T Security Plan: The security of every CS and GSS will be documented in an I/T security plan. Adequate security must be planned for as a normal part of JSC's I/T management process. Planning must include certain areas such as rules for use of the system, requirements for specialized training, personnel and technical controls, and provisions for contingency operations. The reader will find detailed information on how to prepare this plan in section 5.
- c. Periodic Review of Security Controls: The security controls of each CS and GSS must be reviewed at least every three years or upon significant modification to

the system. The scope and frequency of reviews should be commensurate with the acceptable level of risk for the system in question. For systems that have been designated as Special Management Attention systems, these reviews must be done by an independent organization. The reader will find guidance for developing and documenting I/T security controls in sections 4 and 5.

- d. **Authorization to Process:** An appropriate JSC management official must authorize in writing the use of each CS and GSS based upon the implementation of that system's security plan before processing is permitted. If the system has been designated as a special management attention system, then the Authorization to Process must also be signed by the Center CIO. Processing must be re-authorized at least every three years or upon significant change to the system, whichever occurs first. It is extremely important to note that when the line manager signs this certification, that manager is also accepting responsibility for the level of risk inherent in that I/T system. The reader will find guidance in sections 4, and 5 for the analyzing and managing risk.
- e. **I/T Security Awareness and Training:** All individuals who access information in an I/T system operated by or on behalf of the Federal Government shall be trained commensurate with their responsibilities. Training is a required part of the security planning process. The ITSM offers some training for all individuals; system managers must provide some training. Readers will find guidance for I/T security awareness and training in section 7.
- f. **Personnel Security Investigations:** Personnel security is a required part of the security planning process. Every individual who is authorized to bypass I/T security processes and controls must be investigated consistent with the risk or harm that could be caused. It is not a requirement for other users to be investigated. Readers will find guidance in section 8 for identifying and reporting the names of individuals who are required to be investigated as part of the process for granting them access.
- g. **Incident Response:** Within the scope of their duties, all users of I/T systems must be able to recognize an incident, respond to it appropriately, and report it to proper authorities. Readers will find guidance in section 9 for recognizing, responding to, and reporting I/T security incidents.

3.3 I/T SECURITY MANAGEMENT AT THE CENTER LEVEL

3.3.1 Management Review, Evaluation, and Reporting

Periodic review, evaluation, and reporting of I/T security activities are fundamental requirements of the management control of the JSC I/T Security Program. Reports on any aspect of the program are made upon request to NASA Headquarters, the JSC Center Director, or JSC CIO. The contents of these reports are usually derived from the JSC I/T Security Data Base, contractor analyses, OCSM analyses, and from ITSM-sponsored analyses, reviews, and evaluations.

The ITSM is the primary point of contact for release of information regarding JSC's I/T security posture to other Government Agencies and to organizations outside the Government. All such reports will be coordinated with NASA HQS, the JSC Center Director, JSC CIO, and the JSC Office of Public Affairs, as appropriate.

3.3.1.1 METRICS

The goal of the I/T security planning process is to achieve an appropriate level of security in JSC's I/T systems. To that end, at the Center level, JSC's risk management process will be documented by the following four metrics:

- a. Each I/T system under JSC's purview will have a knowledgeable individual assigned responsibility for security.
- b. Each I/T system under JSC's purview will have a published system security plan as described in section 5.
- c. The security controls in each I/T system under JSC's purview will be reviewed every three years or upon significant change to the system, whichever occurs first.
- d. Upon attaining initial operational capability and at least every three years (or upon significant change) thereafter, for each I/T system under JSC's purview, an appropriate line management official must authorize the use of each system in writing before it is permitted to process information.
- e. OCSM's will review the documentation on the systems under their purview at least annually to determine if significant changes have occurred.

Information on these four items will be collected and included in the JSC I/T Security Data Base described in section 3.3.1.2. Because these metrics are prescribed by OMB, they may be the subjects of periodic internal reviews and external audits. The status of these metrics will form the basis of reporting to NASA HQS and to other organizations as required.

3.3.1.2 JSC I/T Security Data Base

Information that the ITSM needs to demonstrate the status of JSC's risk management and reporting activities as well as JSC's adherence to Federal directives is contained in the JSC I/T Security Data Base. The JSC I/T Security Data Base is also considered a quality record under JSC's Quality System. The JSC I/T Security Data Base consists of the following information:

- a. The current roster of names and contact information for the ITSM, DITSM, OCSMs, and Alternate OCSMs
- b. The degree to which each I/T system at JSC has complied with the metrics that were established by OMB Circular A-130, Appendix III, shown by the following elements:

- (1) The name of each I/T system under JSC's cognizance and the type of system (e.g., CS or GSS)
 - (2) For each I/T system, the category or categories of information stored, processed, or transmitted by that system as defined by section 5.4
 - (3) For each I/T system, the name and contact information for the individual responsible for the security of that system
 - (4) For each I/T system, the date of the most recent I/T security plan. For tracking purposes this date is understood to be the date of the last security controls review.
 - (5) For each I/T system, the date that the system was authorized to process sensitive information
 - (6) For each I/T system, the date that the next annual review for significant changes is scheduled to be performed and the date that this annual review expires
 - (7) For each I/T system, its designation as a special management attention system and the reason why it was designated as a special management attention system
- c. Dates, names, and organizational or corporate affiliation of attendees at ITSM-sponsored training.

3.3.1.3 Maintaining the Accuracy and Currency of the JSC I/T Security Data Base

Because the JSC I/T Security Data Base is the primary means of determining JSC's adherence to Federal and Agency I/T security directives, the Data Base must be kept accurate and up-to-date. The following procedure will be used to keep the JSC I/T Security Data Base up to date:

a. Initiating Changes to the Data Base

The OCSMs are responsible for the information contained in their respective organizations' part of the data base and for submitting changes to the JSC I/T Security Data Base. OCSMs will submit changes in writing to a data base administrator as the changes occur. An electronic mail note constitutes a written submission for these purposes. The ITSM will identify the data base administrators to the OCSMs, and these administrators will be the only persons who may make changes to the data base. The data base administrator will make only those changes received in writing from an OCSM. When the data base administrator has made the requested changes, the data base administrator will notify the OCSM in writing that the changes have been made and request that within two working days the OCSM confirm in writing that the requested changes have been correctly entered into the data base.

b. Reviewing Requested Changes

Each OCSM is responsible for the accuracy of the data submitted. The data base administrator will post changes exactly as received. The ITSM will request OCSMs to review their parts of the data base at least annually and send corrections to the data base administrator.

OCSMs, however, should consider frequent reviews of the information for which they are responsible. The data base will be the primary source for reports to Federal Oversight Agencies, NASA HQS, and to the JSC Senior Staff, and no specific data call to the OCSMs will be issued prior to making such reports.

c. Processing Changes to the Data Elements Themselves

The nature of the data collected is driven by Federal and Agency requirements and by the requirements of the JSC Quality System. Only when Federal, Agency, or Quality System guidelines change would the kinds of data collected change.

In the event that Federal, Agency, or Quality System guidelines change, the ITSM will initiate a revision to the data base. New data elements will be determined, and the ITSM will be responsible for developing a plan for transition from old to new data. The ITSM will present the transition plan to the JSC I/T Security Committee and the CIO.

d. Releasing a New or Changed Data Base

The new or changed data base will be released as prescribed by the transition plan.

e. Cancellation

The JSC I/T Security Data Base will remain active with the appropriate elements as long as status of the Center's risk management and reporting activities is required or JSC is required to show compliance with Federal, Agency, or JSC Quality System directives.

f. Changes to This Procedure

This procedure is under the control of the ITSM, and it may be changed as necessary to meet current needs and incorporate new technology. When the procedure is changed, the new procedure will be published as a revised section 3.3.1., and the I/T Security Committee and CIO will be informed.

3.3.1.4 Data base Corrections

Outdated elements in the JSC I/T Security Data Base prevent JSC, not only from conforming to its own Quality System, but also preclude senior management from determining JSC's adherence to Federal and Agency directives. The process described in this section will be invoked when necessary to keep the data base updated.

a. Initial Notification

Normally, initial notification in writing is all that should be necessary. The ITSM will request periodically through the JSC I/T Security Committee that the OCSMs review their current entries in the data base and make changes as necessary. OCSMs will take appropriate action to see that current information described in section 3.3.1.2 above is presented in writing to a data base administrator.

b. Lack of Response to Initial Notification

If the organization does not respond to the initial notification, the ITSM will notify the OCSM individually. The affected OCSM and ITSM will mutually agree upon an appropriate response and schedule to ensure that the appropriate security planning products have been issued and that they are reflected in the data base.

No response within one month of individual notification will be cause for the ITSM to notify the JSC CIO.

The JSC CIO will advise the corresponding Senior Staff member in writing (an electronic mail note constitutes notification in writing for the purposes of this process). This notification will include a request that the affected OCSM contact the ITSM so that they may work out an appropriate schedule.

The ITSM will keep the JSC CIO periodically apprised of progress and adherence to schedule.

c. Failure to Maintain Scheduled Progress

In the event that progress still is not made, the ITSM will issue a JSC Corrective Action Request (JCAR) under the JSC Quality Management System. The process described in the current version of JSC System Level Procedure (SLP) 4-14.1, *Corrective Action*, will be followed.

d. Appeal to the Center Director

Because the information in the JSC I/T Security Data Base is collected pursuant to Federal and Agency directives, security planning is mandatory. Therefore, if the JSC Corrective Action process still does not result in the required information being furnished, the ITSM will report this fact to the JSC CIO who will request the JSC Center Director to intervene.

3.3.2 ITSM-Sponsored Analyses, Reviews, and Evaluations

The ITSM may conduct at any time independent analyses, reviews, or evaluations of any I/T system under JSC's purview. An analysis, review, or evaluation may be requested by the Center Director, CIO, ITSM, OCSM, or the organization's management chain. The requester and the ITSM will agree in advance upon the scope of the activity. The activity may focus upon any aspect of the target system's security, but must incorporate an automated or manual penetration test. Because

the difference between a penetration test and an unauthorized external intrusion may be no more than management concurrence, special rules for penetration testing have been established which the reader will find in section 10.5.

A security analysis may consist of any or all of the following components as circumstances dictate:

- a. Automated or manual penetration testing
- b. Review of system documentation, including problem reports, plans, and schedules
- c. Interviews with system personnel
- d. Examination of the target system's physical security

The ITSM will not conduct any analysis, without notification to the management chain to which the target system belongs, including the OCSM. It is solely the option of the target system's management chain to determine how much notice is given to other concerned employees.

The ITSM may conduct other reviews and evaluations as needed by convening self-assessment teams or other small groups as appropriate to the issue being investigated.

3.3.3 The JSC I/T Security Engineering Team

The Security Engineering Team works under the operational control of the DITSM. The team consists solely of civil servants who are required to maintain a minimum of a SECRET security clearance. Upon request of an appropriate JSC management official, the ITSM will assign this team to conduct the analysis, review, or evaluation. The team provides an effective, independent report on any aspect of an I/T system's security. The team will use many tools to gather results, but the most important among them is penetration testing.

While the analysis that the team conducts includes some elements of a traditional risk analysis, this independent analysis, review, or evaluation does not replace the requirement for a continuing risk management program for the target system. The analysis only provides a "snapshot" at a given point in time that is only valid for the security aspects of the system that are the subject of the test. However, the system's line manager may use the team's report as a foundation for ongoing self-assessment.

Reports that the JSC Security Engineering Team generates are considered sensitive information; neither the ITSM nor the team will distribute them further. The team provides the final report to the manager who requested the test and to the ITSM. Only the responsible line manager may provide copies to other personnel.

3.4 OCSMs' ANNUAL REVIEW OF I/T SECURITY PROGRAM IN THE ORGANIZATION

At least annually the OCSM from each JSC organization will review the I/T security program for that organization. At a minimum, the following must be included in the review:

- a. Identification of the I/T systems to assess what, if any, changes have occurred
- b. Changes in designation of each of the I/T systems as CS or GSS.
- c. Categories of information processed by each of the systems remains correct
- d. Training of personnel is and will remain adequate.
- e. Required personnel security investigations have been accomplished.
- f. An effective incident reporting process is in place and functioning.

A report of the review and evaluation will be given to the director or office chief as appropriate. Additionally, changes and deficiencies will be reported to the ITSM. When the review has been completed to the OCSM's satisfaction, the OCSM should report the review complete to the JSC I/T Security Data Base Administrator in writing. The Data Base Administrator will update the annual review due date.

3.5 REVIEWS BY INDIVIDUAL JSC ORGANIZATIONS

In addition to the activities prescribed by this handbook, JSC organizations are encouraged to conduct proactive I/T security programs if the risks to their assets are sufficiently great. Organizations may:

- a. Conduct their own analyses, reviews, and evaluations, including penetration testing, provided they follow the penetration testing guidelines specified in section 10.
- b. Issue written supplements to the requirements and guidelines of this handbook if necessary, although to avoid duplication of effort, organizations are encouraged to use this handbook as the sole reference.
- c. Impose more (but never less) stringent I/T security requirements than are found in this handbook if a risk analysis indicates the need to do so.

3.6 PERSONNEL SECURITY INVESTIGATIONS

Federal guidelines in effect at the time this handbook is published require personnel to be investigated whose access privileges are such that they can bypass I/T security processes and controls. Only the JSC Security Branch is authorized to conduct personnel security investigations. The sole duty that line managers have under the JSC I/T Security Program is to identify those individuals who require investigations and to furnish their names to the JSC Security Branch. Section 8 of

this handbook provides guidance on how to identify and submit those individuals for investigation. Managers should note that recent changes in the Federal guidelines have eliminated their ability to accept risk. That is, if the person needs an investigation at all, that investigation must be completed favorably before the employee is permitted to have privileged access. **Line managers no longer may accept the risk** of granting privileged access while the investigation is being processed.

3.7 I/T SECURITY AWARENESS AND TRAINING

Certain training is common to everyone in the JSC community. Subject to availability of resources, the ITSM will provide some of the common training, particularly when similar products need to be produced in a common format Centerwide. The ITSM will provide classes in risk analysis leading to the preparation of system security plans and an understanding of the I/T system's life-cycle security responsibilities. Also provided will be periodic classes and seminars on security topics of interest Centerwide. OCSMs and system security administrators are required to take at least the I/T security planning class.

The ITSM will keep a record of the training that is offered at the Center level. This record will consist of name of the class, date(s), names and organizational affiliations of the students that completed the training successfully.

There is, however, a great deal of system-specific and organization-specific training that the ITSM cannot provide. The organization in question is responsible for that training. Each JSC contractor is responsible for ensuring that their personnel are properly trained in their I/T security responsibilities.

The minimum requirement for periodic I/T security awareness and training is met for to all civil servants and on-site contractors via the Annual Security Refresher Briefing. This refresher training is supported by agreement with the JSC Security Branch.

3.8 CONFIGURATION MANAGEMENT OF THIS HANDBOOK

The current edition of this handbook is available from the AI Master List of documents in the JSC Quality System. The electronic edition found on the AI Master List is the current version. This handbook will be updated periodically as JSC's threats, vulnerabilities, and technologies change. To maintain the accuracy and authenticity of the handbook, the following configuration management process will be used:

3.8.1 Initiating a New Document or Initiating Changes to the Existing Document

Requests for a new document, changes to the existing document, or cancellation of the document at the end of its life are submitted in writing to the ITSM who is the document owner. Electronic mail, fax, or hard copy are all acceptable media for

requesting a change. A specific form is not required, but the requester must provide a clear statement of the action desired.

All requests for change will be filed separately in a location marked for document changes.

3.8.2 Reviewing Requested Changes

The ITSM is responsible for periodically taking all changes to the JSC I/T Security Committee for review and recommended dispositions of requested changes.

3.8.3 Processing the Handbook and Proposed Changes to the Handbook

After the JSC I/T Security Committee has reviewed all proposed changes, their recommendations will be presented to the I/T Steering Council for its approval. The ITSM submits the proposed final version to the JSC CIO for review and signature.

3.8.4 Releasing a New or Changed Handbook

The revised and approved document is presented to the AI Master List Custodian in electronic form. The AI Master List Custodian will update the AI Master List and provide the document for posting to the JSC Quality System Electronic Document Repository in accordance with the instructions contained in the current version of JSC 27688, *Master List Instructions*, as prescribed by SLP 4.5.

After the document has been posted on the JSC Quality System Electronic Document Repository, the ITSM will ensure that the posted version is the correct one. This version then becomes the current edition.

3.8.5 Cancellation of this Handbook

Cancellation of this handbook may be requested in accordance with section 3.8.1. The ITSM will process requests for cancellation as any other document change using the procedures for reviewing, processing, and releasing processed.

When the ITSM and the CIO have approved cancellation, the ITSM will notify the AI Master List Custodian in writing. Electronic mail, fax, or hard copy all fulfill the requirement for notification in writing.

The AI Master List Custodian will then advise the JSC Quality System Electronic Documents Repository Custodian in writing (electronic mail, fax, or hard copy) that the handbook is been canceled and will follow the process for removing a document from the JSC Quality System document management system as described in JSC 27688, *Master List Instructions* as prescribed by SLP 4.5.

The ITSM will ensure that the document has been removed from the JSC Quality System Electronic Document Repository.

SECTION 4

INTRODUCTION TO I/T SYSTEM SECURITY ENGINEERING

4.0 INTRODUCTION TO I/T SYSTEM SECURITY ENGINEERING

This section presents a complete end-to-end overview of the entire I/T security planning process. The reader will find a complete overview of the risk analysis process followed by a discussion of how the risk analysis is used to prepare the security planning documents. This section does not present the details of how to assess risks and prepare security plans; the reader will find these processes in section 5.

The purpose of the discussion is to reinforce the point that every step in the life cycle process of designing, acquiring, operating, upgrading, and finally disposing of an I/T system at the end of its useful life has a security component embedded in it.

Central to every step of a project's life cycle is the idea of assessment and management of risk. To have a risk, two conditions are required: a threat must exist, and the system must be vulnerable to that threat. If one or the other is absent, there is no risk. By evaluating, prioritizing, and making wise decisions about which risks to accept, and in what degree, as the planning, acquisition, implementation, and operations proceed, a manager gains as much control as desired (or as the budget allows) over the integrity, availability, and confidentiality of the information in the system.

There are two ideas behind the risk-based approach to I/T security. First is the notion of cost effectiveness. If a system line manager only has to spend money to protect a system against the threats to which the system is vulnerable, the controls will almost certainly cost less for any given level of security. During the years in which JSC conducted classified Space Shuttle operations, the Center retrofitted security controls for classified information on its I/T systems at enormous cost. The nature of the threats was decided elsewhere, and vulnerabilities were assumed simply because the threats existed. The most important lesson JSC learned from that experience was that the only cost-effective way to provide security for its unclassified operations was to place the responsibility in the hands of the line manager and to let the concerned manager determine and analyze the risks, manage the risks, and be responsible for the outcome. Thus, the second idea behind the risk-based approach is that of management responsibility. Within reasonable limits, line managers may accept the degree of risk that their analysis and budgets dictate so long as they understand that they are fully accountable for the outcome of their decisions. To accept risk intelligently, managers must understand the risk analysis process and understand the potential impacts of accepting too much risk, including exposing NASA to unacceptable liabilities, exposing themselves to potential civil or criminal penalties, or posing an undue risk to others who share the common resources—considerations all too frequently not in the manager's mind during risk acceptance.

4.1 OVERVIEW OF THE I/T SECURITY PLANNING PROCESS

A manager must understand the risks to which the system is subject in order to select and impose appropriate security controls. Only from a risk analysis can a line manager prepare an adequate security plan. Although Federal and Agency directives no longer require risk analyses to be published, the risk analysis is still the foundation of the security plan. An appropriate I/T security plan must be published for every I/T system.

The I/T security plan is the logical end of a well-established security planning process. A reader seeking an overview and description of the steps in the security planning process without the details will find the overview in this section. The process consists of ten steps, as follows:

- a. Determination of the boundaries of the system that will be analyzed.
- b. Assignment of the system as either a critical system or a general support system as defined in section 3.1.
- c. Analysis of the applications and data to be processed in the system in order to assign a system to one of the information categories defined in section 5.3.
- d. Risk analysis.
- e. Risk reduction analysis.
- f. Management decision.
- g. Risk reduction actions.
- h. Implementation and maintenance of safeguards throughout the system's life cycle.
- i. Ensuring supporting functions such as I/T security awareness and training, personnel security investigations, and incident recognition/reporting/response are accomplished.
- j. Completion of I/T security metrics; i.e., assignment of responsibility for security, publication of a security plan, periodic review of security controls, and granting authorization to process.

A discussion of each of these steps follows.

4.2.1 Determination of System Boundaries

The first step in the I/T security planning process is to determine the boundaries of the system that is to be the subject of the analysis that follows. The importance of this step is often unappreciated. It is the only way to determine the elements that constitute the system, how the users will interface with the system (and what their special needs are, if any), and who is responsible for the system. The reader should

recall from the discussion in section 3.1 that a *system* may mean an I/T system in the traditional sense (hardware, software, facilities) or may be an application or bundle of similar applications—they will be treated the same for I/T security planning purposes. This step also establishes the intended limits of liability for the responsible line manager as well as permits the line manager to divide the I/T resources into reasonable management units.

4.2.2 Assignment as a Critical System or General Support System

A list of critical systems is given in section 5.2.1. For the purposes of this section, the reader should understand that all Federal I/T systems fall into two categories, *critical systems*, whose distinguishing characteristic is the need for special management attention to security due to the criticality of the system to the Agency's mission, and *general support systems* that includes all other I/T systems. The distinction is important because of the catastrophic effects that may accrue to NASA if information in a critical system is altered, made unavailable, or improperly disclosed. Section 5.3 provides the reader with all the information needed to establish the category to which any given system belongs.

4.2.3 Assignment of One or More Information Categories

All information that is contained in JSC's I/T systems falls under one of the five categories defined in detail in section 5.3. All information in a Government I/T system is considered sensitive to some degree and is entitled to an appropriate level of protection. By assigning the system to one of the categories, a manager has some idea of the type and stringency of controls that will be required.

The reader should note that there is no restriction to storing, processing, or transmitting several categories of sensitive information in the same I/T system. The responsible manager's obligation is to know what kinds of information are there and to provide the appropriate I/T security controls for that information.

4.2.4 Risk Analysis

Risk analysis is the foundation of the I/T security planning process. In this step, a manager determines the system threats and vulnerabilities, prioritizes the risks, and inventories available security controls that would mitigate or correct the risks. Risk analysis consists of the following steps:

- a. Identification of the assets that are at risk—these are the assets within the boundary defined previously.
- b. Determination of replacement value of those assets and resources.
- c. Identification of the threats to the assets at risk.
- d. Identification of the vulnerabilities that might allow the threats to be realized.

- e. Identification of vulnerabilities that this I/T system, should it go into operation as planned, could produce for others who share common resources.
- f. Determining and prioritizing the risks.
- g. Identification of available controls.

4.2.5 Risk Reduction Analysis

Risk reduction analysis is the step by which a manager, knowing the risks and having listed the controls already available, now addresses what additional controls are needed to bring the risks to a manageable level. The output of this step is a set of recommendations for additional security controls. Risk reduction analysis consists of the following steps:

- a. Identification of potential additional security controls.
- b. Determination of the operational feasibility and life-cycle costs of the potential security controls, including controls that will prevent or mitigate risks to others who share common resources.
- c. Preparation of risk analysis and risk reduction recommendations, including alternative solutions, for presentation to management.

4.2.6 Management Decision

In this step, the responsible line manager decides which risks to correct, which can only be mitigated, and which must be accepted. JSC line managers are responsible for determining acceptable levels of risk to their systems. Risk acceptability is usually based upon cost/benefit estimates, technical or operational constraints, the feasibility of implementing the safeguards, or the availability of safeguards. In the real world, some risk, called the **residual risk**, will always remain. Line managers must be sure that they can live with the residual risk that they have chosen.

The responsible line manager now makes the final selection of I/T security controls and determines the implementation priorities. These actions are embodied in the next step.

4.2.7 Risk Reduction Actions

Once JSC line management has decided which I/T security controls are to be implemented and the order of priority for installation, the actual implementation begins. The size and complexity of the task dictate whether or not a formal risk reduction action plan should be written. In many cases, the risk analysis will show that no security controls other than physical controls, good procedures, and those technical controls furnished by the system's manufacturer need be implemented in order to reduce the risks to a manageable level.