



WHITE PAPER



COMPLIANT SOLUTIONS

MAPPING OF CARPATHIA GOVERNMENT SOLUTIONS HOSTING
CAPABILITIES TO MODERATE IMPACT CONTROLS OF NIST 800-53

CONTENTS

OVERVIEW	3
Carpathia Government Solutions	
Capabilities to NIST 800-53, Revision 3	3
Key/Definitions	3
MAPPING OF CARPATHIA MANAGED HOSTING CAPABILITIES TO	
MODERATE LEVEL CONTROLS OF NIST 800-53, REVISION 3	4
Access Control	4
Awareness & Training	5
Audit & Accountability	5
Certification, Accreditation & Security Assessments	6
Configuration Management	6
Contingency Planning	7
Identification & Authentication	7
Incident Response	8
Maintenance	8
Media Protection	9
Physical & Environmental Protection	9
Planning	10
Personnel Security	10
Risk Assessment	11
Systems & Services Acquisition	11
System & Communications Protection	12
Program Management	14
SECURITY CONTROL BASELINES – SUMMARY	15
Low-Impact, Moderate-Impact and High-Impact Information Systems	15
MINIMUM ASSURANCE REQUIREMENTS	16
Low-Impact, Moderate-Impact and High-Impact Information Systems	16
ABOUT CARPATHIA GOVERNMENT SOLUTIONS	18

OVERVIEW

CARPATHIA GOVERNMENT SOLUTIONS CAPABILITIES TO NIST 800-53 REVISION 3

The table on the following page has been excerpted from 800-53 rev.3 and adapted by Carpathia Government Solutions (CGS) to include two coded columns on the left-hand side.

The first shows activities at the system level, and the second shows those at the application level. The color coded shapes indicate the responsibility assumed by the respective parties and are defined in the key below.

KEY/DEFINITIONS

	DEFINITION	DETAIL
✓	At system level, Carpathia provides.	Carpathia has all capabilities in-house to perform. If agency elects to delegate this function to Carpathia, we can provide since it is part of our regular processes. Alternatively, agency can retain full responsibility.
+	Requirements not mandated at "Moderate," but Carpathia meets specification regardless.	Carpathia meets the specification at "Moderate" level of control, even though it is not required.
○	Application level responsibility that is strongly dependent on agency or developer	Agency or outside developer is responsible.
●	Oversight or governance-related responsibility	Typically procedural/governance in nature (i.e. PL-5, privacy impact assessment). Agency must perform. Carpathia cannot perform or otherwise be involved, because agency has full responsibility by law.
◇	System-level responsibility that is strongly dependent on application details	Requirement typically cannot be outsourced. Application-level is agency responsibility.

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ○ Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

MAPPING OF CARPATHIA MANAGED HOSTING CAPABILITIES TO MODERATE LEVEL CONTROLS OF NIST 800-53, REVISION 3

ACCESS CONTROL							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
◇		AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
✓		AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
✓	●	AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
✓		AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
✓		AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
✓	●	AC-7	Unsuccessful Login Attempts	P1	AC-7	AC-7	AC-7
✓	●	AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
✓	●	AC-9	Previous Logon Notification	P0	Not Selected	Not Selected	Not Selected
✓	●	AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
✓	●	AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
✓	●	AC-12	Session Termination (Withdrawn)	---	---	---	---
◇		AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---
✓	●	AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14 (1)	AC-14 (1)
N/A (high risk only)	N/A (high risk only)	AC-15	Automated Marking (Withdrawn)	---	---	---	---
N/A	N/A	AC-16	Automated Labeling	P0	Not Selected	Not Selected	Not Selected
✓		AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4) (5) (7) (8)	AC-17 (1) (2) (3) (4) (5) (7) (8)
✓		AC-18	Wireless Access Restrictions	P1	AC-18	AC-18 (1)	AC-18 (1) (2) (4) (5)
✓		AC-19	Access Control for Portable and Mobile Systems	P1	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
✓		AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
N/A	N/A	AC-21	User-Based Collaboration and Information Sharing	P0	Not Selected	Not Selected	Not Selected
	●	AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

AWARENESS & TRAINING							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
✓		AT-2	Security Awareness	P1	AT-2	AT-2	AT-2
✓		AT-3	Security Training	P1	AT-3	AT-3	AT-3
✓		AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
✓		AT-5	Contacts with Security Groups and Associations	P0	Not Selected	Not Selected	Not Selected

AUDIT & ACCOUNTABILITY							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
✓	●	AU-2	Auditable Events	P1	AU-2	AU-2 (3) (4)	AU-2 (3) (4)
✓	●	AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
✓	●	AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
✓	●	AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
◇		AU-6	Audit Monitoring, Analysis, and Reporting	P1	AU-6	AU-6	AU-6 (1)
◇		AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
✓	●	AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
✓		AU-9	Protection of Audit Information	P1	AU-9	AU-9	AU-9
N/A	N/A	AU-10	Non-repudiation	P1	Not Selected	Not Selected	AU-10
N/A		AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
✓		AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1)
N/A	N/A	AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
N/A	N/A	AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

CERTIFICATION, ACCREDITATION & SECURITY ASSESSMENTS							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	P1	CA-1	CA-1	CA-1
	●	CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
✓		CA-3	Information System Connections	P1	CA-3	CA-3	CA-3
	◊	CA-4	Security Certification (Withdrawn)	---	---	---	---
✓	◊	CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
	◊	CA-6	Security Accreditation	P3	CA-6	CA-6	CA-6
✓		CA-7	Continuous Monitoring	P3	CA-7	CA-7	CA-7

CONFIGURATION MANAGEMENT							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
✓		CM-2	Baseline Configuration and System Component Inventory	P1	CM-2	CM-2 (1) (3) (4)	CM-2 (1) (2) (3) (5) (6)
✓		CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
✓		CM-4	Monitoring Configuration Changes	P2	CM-4	CM-4	CM-4 (1)
✓		CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
	◊	CM-6	Configuration Settings	P1	CM-6	CM-6 (3)	CM-6 (1) (2) (3)
✓		CM-7	Least Functionality	P1	CM-7	CM-7 (1)	CM-7 (1) (2)
✓		CM-8	Information System Component inventory	P1	CM-8	CM-8 (1) (5)	CM-8 (1) (2) (3) (4) (5)
✓		CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ◊ Application level responsibility ● Agency must perform ◊ Not provided by CGS at the system level

CONTINGENCY PLANNING							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓	●	CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
✓	●	CP-2	Contingency Plan	P1	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
	●	CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
✓		CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
---	---	CP-5	Contingency Plan Update (Withdrawn)	---	---	---	---
✓		CP-6	Alternate Storage Sites	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
✓	●	CP-7	Alternate Processing Sites	P1	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
✓		CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
✓		CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
◇		CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)

IDENTIFICATION & AUTHENTICATION							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
✓		IA-2	User Identification and Authentication	P1	IA-2 (1)	IA-2 (1) (2) (3) (8)	IA-2 (1) (2) (3) (4) (8) (9)
✓		IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
✓		IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
✓		IA-5	Authenticator Management	P1	IA-5 (1)	IA-5 (1) (2) (3)	IA-5 (1) (2) (3)
✓		IA-6	Authenticator Feedback	P1	IA-6	IA-6	IA-6

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

✓		IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
✓		IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8	IA-8	IA-8

INCIDENT RESPONSE

CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
✓	●	IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)
✓	●	IR-3	Incident Response Testing	P2	Not Selected	IR-3	IR-3 (1)
✓		IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1)
✓		IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
✓		IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
✓		IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
✓		IR-8	Incidence Response Plan	P1	IR-8	IR-8	IR-8

MAINTENANCE

CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
✓		MA-2	Periodic Maintenance	P2	MA-2	MA-2 (1)	MA-2 (1) (2)
✓		MA-3	Maintenance Tools	P2	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
✓		MA-4	Remote Maintenance	P1	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
✓		MA-5	Maintenance Personnel	P1	MA-5	MA-5	MA-5
✓		MA-6	Timely Maintenance	P1	Not Selected	MA-6	MA-6

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

MEDIA PROTECTION							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
✓		MP-2	Media Access	P1	MP-2	MP-2 (1)	MP-2 (1)
✓		MP-3	Media Labeling	P1	Not Selected	MP-3	MP-3
✓		MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
✓		MP-5	Media Transport	P1	Not Selected	MP-5 (2) (4)	MP-5 (2) (3) (4)
✓		MP-6	Media Sanitization and Disposal	P1	MP-6	MP-6	MP-6 (1) (2) (3)

PHYSICAL & ENVIRONMENTAL PROTECTION							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
✓		PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
✓		PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
+		PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
✓		PE-5	Access Control for Display Medium	P1	Not Selected	PE-5	PE-5
✓		PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (2)
✓		PE-7	Visitor Control	P1	PE-7	PE-7 (1)	PE-7 (1)
✓		PE-8	Access Records	P3	PE-8	PE-8	PE-8 (1) (2)
✓		PE-9	Power Equipment and Power Cabling	P1	Not Selected	PE-9	PE-9
✓		PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
✓		PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
✓		PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
✓		PE-13	Fire Protection	P1	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
✓		PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
✓		PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
✓		PE-16	Delivery and Removal	P1	PE-16	PE-16	PE-16

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

✓		PE-17	Alternate Work Site	P1	Not Selected	PE-17	PE-17
✓		PE-18	Location of Information System Components	P2	Not Selected	PE-18	PE-18 (1)
+		PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected

PLANNING							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓	○	PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
✓	○	PL-2	System Security Plan	P1	PL-2	PL-2	PL-2
---	---	PL-3	System Security Plan Update (Withdrawn)	---	---	---	---
✓		PL-4	Rules of Behavior	P1	PL-4	PL-4	PL-4
	●	PL-5	Privacy Impact Assessment	P1	PL-5	PL-5	PL-5
✓		PL-6	Security-Related Activity Planning	P3	Not Selected	PL-6	PL-6

PERSONNEL SECURITY							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓		PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
✓		PS-2	Position Categorization	P1	PS-2	PS-2	PS-2
✓		PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
✓		PS-4	Personnel Termination	P2	PS-4	PS-4	PS-4
✓		PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
✓		PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
✓		PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
✓		PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8

- ✓ At system level, Carpathia provides
- Application level responsibility
- Agency must perform
- ✚ Not required at "Moderate," but CGS meets specification
- ◇ Not provided by CGS at the system level

RISK ASSESSMENT							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓	○	RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
✓	○	RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
✓	○	RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
---		RA-4	Risk Assessment Update (Withdrawn)	---	---	---	---
✓	○	RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1)	RA-5 (1) (2) (3) (4) (5) (7)

SYSTEMS & SERVICES ACQUISITION							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
	○	SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
	○	SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
✓	○	SA-3	Life Cycle Support	P1	SA-3	SA-3	SA-3
	○	SA-4	Acquisitions	P1	SA-4	SA-4 (1) (4)	SA-4 (1) (2) (4)
✓	○	SA-5	Information System Documentation	P2	SA-5	SA-5 (1) (3)	SA-5 (1) (2) (3)
✓	○	SA-6	Software Usage Restrictions	P1	SA-6	SA-6	SA-6
	○	SA-7	User Installed Software	P1	SA-7	SA-7	SA-7
	○	SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
✓	○	SA-9	Outsourced Information System Services	P1	SA-9	SA-9	SA-9
		SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
	○	SA-11	Developer Security Testing	P2	Not Selected	SA-11	SA-11
✓		SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
✓		SA-13	Trustworthiness	P1	Not Selected	Not Selected	SA-13
✓		SA-14	Critical Information System Components	P0	Not Selected	Not Selected	Not Selected

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ○ Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

SYSTEM & COMMUNICATIONS PROTECTION							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓	●	SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
✓	●	SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
✓		SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
✓	●	SC-4	Information Remnants	P1	Not Selected	SC-4	SC-4
✓		SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
✓		SC-6	Resource Priority	P0	Not Selected	Not Selected	Not Selected
✓		SC-7	Boundary Protection	P1	SC-7	SC-7 (1) (2) (3) (4) (5) (7)	SC-7 (1) (2) (3) (4) (5) (6) (7) (8)
✓	●	SC-8	Transmission Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
✓	●	SC-9	Transmission Confidentiality	P1	Not Selected	SC-9 (1)	SC-9 (1)
✓		SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
N/A	N/A	SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
✓	●	SC-12	Cryptographic Key Establishment and Mgmt.	P1	SC-12	SC-12	SC-12 (1)
✓	●	SC-13	Use of Validated Cryptography	P1	SC-13	SC-13	SC-13
	●	SC-14	Public Access Protections	P1	SC-14	SC-14	SC-14
✓	●	SC-15	Collaborative Computing	P1	SC-15	SC-15	SC-15
N/A	N/A	SC-16	Transmission of Security Parameters	P0	Not Selected	Not Selected	Not Selected
✓	●	SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
	●	SC-18	Mobile Code	P1	Not Selected	SC-18	SC-18
	●	SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
◇		SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20 (1)	SC-20 (1)	SC-20 (1)
N/A (high risk only)	N/A (high risk only)	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	Not Selected	Not Selected	SC-21

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

		SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	Not Selected	SC-22	SC-22
✓	●	SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
		SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
N/A	N/A	SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
N/A	N/A	SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
N/A	N/A	SC-27	Operating System-Independent Applications	P0	Not Selected	Not Selected	Not Selected
		SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
✓		SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
		SC-30	Virtualization Techniques	P0	Not Selected	Not Selected	Not Selected
	●	SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
✓		SC-32	Information System Partitioning	P1	Not Selected	SC-32	SC-32
✓	●	SC-33	Transmission Preparation Integrity	P0	Not Selected	Not Selected	Not Selected
✓		SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected

SYSTEM & INFORMATION INTEGRITY							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINE		
SYS LEVEL	APP LEVEL				LOW	MOD	HIGH
✓	●	SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
◇		SI-2	Flaw Remediation (patch management)	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
◇		SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2) (3)	SI-3 (1) (2) (3)
✓		SI-4	Information System Monitoring Tools and Techniques	P1	Not Selected	SI-4 (2) (4) (5) (6)	SI-4 (2) (4) (5) (6)
N/A (high risk only)	N/A (high risk only)	SI-5	Security Alerts and Advisories	P1	SI-5	SI-5	SI-5 (1)
N/A (high risk only)	N/A (high risk only)	SI-6	Security Functionality Verification	P1	Not Selected	Not Selected	SI-6
		SI-7	Software and Information Integrity	P1	Not Selected	SI-7 (1)	SI-7 (1) (2)
		SI-8	Spam Protection	P1	Not Selected	SI-8	SI-8 (1)
✓	●	SI-9	Information Input Restrictions	P2	Not Selected	SI-9	SI-9

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ● Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

		SI-10	Information Accuracy, Completeness, Validity, and Authenticity	P1	Not Selected	SI-10	SI-10
	○	SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
✓	○	SI-12	Information Output Handling and Retention	P2	SI-12	SI-12	SI-12
✓		SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected

PROGRAM MANAGEMENT							
CGS MEETS MODERATE SPECS AT		CNTL NO.	CONTROL NAME	PRIORITY			
SYS LEVEL	APP LEVEL						
N/A	N/A	PM-1	Information Security Program Plan	P1			
N/A	N/A	PM-2	Senior Information Security Officer	P1			
N/A	N/A	PM-3	Information Security Resources	P1			
N/A	N/A	PM-4	Plan of Action and Milestones Process	P1			
N/A	N/A	PM-5	Information System Inventory	P1			
N/A	N/A	PM-6	Information Security Measures of Performance	P1			
N/A	N/A	PM-7	Enterprise Architecture	P1			
N/A	N/A	PM-8	Critical Infrastructure Plan	P1			
N/A	N/A	PM-9	Risk Management Strategy	P1			
N/A	N/A	PM-10	Security Authorization Process	P1			
N/A	N/A	PM-11	Mission/Business Process Definition	P1			

✓ At system level, Carpathia provides + Not required at "Moderate," but CGS meets specification
 ○ Application level responsibility ● Agency must perform ◇ Not provided by CGS at the system level

Supporting Information Excerpted from NIST 800-53A, Rev. 3

SECURITY CONTROL BASELINES — SUMMARY

Low-Impact, Moderate-Impact and High-Impact Information Systems

This appendix contains the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems.⁷¹ The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.⁷² If a security control is selected for one of the baselines, the security control family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked “not selected.” Control enhancements, when used to supplement security controls, are indicated by the number of the control enhancement. For example, an “IR-2 (1)” in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Note that some security controls and enhancements in the security control catalog are not used in any of the baselines in this appendix but are available for use by

organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risk to organizational operations and organizational assets, individuals, other organizations, and the Nation.

Organizations can use the recommended priority code designation associated with each security control in the baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 (P2) control has a higher priority for implementation than a Priority Code 3 [P3] control). This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until all of the security controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions. Table D-1 summarizes sequence priority codes for the baseline security controls in Table D-2.

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

PRIORITY CODE	SEQUENCING	CONTROL NAME
Priority Code 1 (P1)	FIRST	Implement P1 security controls first
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls
Unspecified Priority Code (P0)	NONE	Security control not selected for baseline

71. A complete description of all security controls is provided in Appendices F and G. In addition, separate documents for individual security control baselines (listed as Annexes 1, 2, and 3) are available at <http://csrc.nist.gov/publications>.

72. The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., CP-4 Contingency Plan Testing and Exercises—Moderate: CP-4 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g. CP-4 Contingency Plan Testing and Exercises – Low: CP-4.)

MINIMUM ASSURANCE REQUIREMENTS

Low-Impact, Moderate-Impact and High-Impact Information Systems

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers⁷³ define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by information system impact level (i.e., low, moderate, and high) since the requirements apply to each control within the respective impact level. Using a format similar to security controls, assurance requirements are followed by supplemental guidance that provides additional detail and explanation of how the requirements are to be applied. Bolded text indicates requirements that appear for the first time at a particular impact level.

Low-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement.

Supplemental Guidance: For security controls in low-impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Moderate-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description**

of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in moderate-impact information systems, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

Note: This level of assurance is not intended to protect a moderate-impact information system against high-end threat agents (i.e., threat agents that are highly skilled, highly motivated, and well-resourced). When such protection is required, the section below entitled *Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems* applies.

High-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis and testing of the control **(including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific

⁷³ In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls. This may include in addition to organizational personnel, for example, hardware and software vendors providing the controls and contractors implementing the controls.

actions supporting increased confidence that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in high-impact information systems, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Note: This level of assurance is not intended to protect a high-impact information system against high-end threat agents (i.e., threat agents that are highly skilled, highly motivated, and well-resourced). When such protection is required, the section below entitled Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems applies.

Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for moderate-impact and high-impact information systems, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

ABOUT CARPATHIA GOVERNMENT SOLUTIONS

Carpathia Government Solutions (CGS) is the leading provider of federally-compliant managed hosting services for government agencies and businesses. For over ten years, our mission has been to deliver, protect, and defend our customer’s most important applications and data in a manner that is fully compliant with a superset of federal security standards. We achieve this by providing our customers a complete managed hosting solution that spans the full range of IT requirements in our pioneering, highly-secure and federally-compliant data center. Every aspect of our solution from the facility to the network to the systems we support is backed by our experience, knowledge and the time-tested procedures that have resulted in 100% certification and accreditation (C&A) under FISMA and DIACAP guidelines for our customers.

Our key differentiator is our ability to design, build and manage highly-complex environments quickly, reliably, and per federal security requirements including FISMA, DIACAP, and agency-specific mandates.

Understanding that every federal hosted environment is required to meet specific security requirements, our branded delivery model, Federally Compliant Application Platform (FCAP), is an IT infrastructure built from the ground up to be 100% compliant with a superset of federal mandates. Government agency applications deploying on the FCAP platform inherit the compliance-based disciplines and uniform delivery postures that enable us to guarantee 100% C&A up to the application layer.

Examples of current Federal Agency customers for which Carpathia Government Solutions has official Authority to Operate (ATO) include, but are not limited to:



DEFENSE



HOMELAND SECURITY



INTELLIGENCE



CIVILIAN

Carpathia Hosting is a leading provider of managed hosting services, delivering secure, reliable and compliant IT infrastructure and management for some of the world’s most demanding enterprises and federal agencies. Founded in 2003, Carpathia is a growing, profitable business run by a seasoned management team with deep experience in delivering enterprise hosting solutions including colocation, managed services and cloud computing. Carpathia’s suite of services is designed for organizations seeking scalable, secure, robust and enterprise-grade hosting solutions that can be quickly provisioned or tailored to meet unique requirements. Backed by its E3 Promise, Carpathia consistently delivers an experience that exceeds customers’ expectations. Carpathia qualifies as a small business. Contact Carpathia at 1.888.200.9494, or visit www.carpathia.com for more information. References to other products are made to show compatibility. All companies and/or products mentioned in this document are registered or trademarked by their respective organizations. The inclusion of third party products does not infer endorsement by these parties, unless otherwise noted.