NIST SP 800-53 (Rev 4)			Cybersecurty Framework
No.	Control	Yr Priority	
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	y1	AC-1
AC-2	ACCOUNT MANAGEMENT	y1	AC-2
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	y1	AC-7
AC-17	REMOTE ACCESS	y1	AC-17
AC-18	WIRELESS ACCESS	y1	AC-18
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	y1	AT-1
AT-3	ROLE-BASED SECURITY TRAINING	y1	AT-3
CA-5	PLAN OF ACTION AND MILESTONES	y1	CA-5 (Added)
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	y1	PE-1
PL-4	RULES OF BEHAVIOR	y1	PL-4 (Added)
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	y1	PS-1
PS-4	PERSONNEL TERMINATION	y1	PS-4
SC-13	CRYPTOGRAPHIC PROTECTION	y1	SC-13
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	y1	SI-1
SI-2	FLAW REMEDIATION	y1	SI-2
SI-3	MALICIOUS CODE PROTECTION	y1	SI-3
AC-3	ACCESS ENFORCEMENT	y1	AC-3
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	y1	IA-1
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	y1	IA-2
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	y1	IR-1
IR-6	INCIDENT REPORTING	y1	IR-6
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	y1	MP-1
MP-2	MEDIA ACCESS	y1	MP-2
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	y1	RA-1
RA-2	SECURITY CATEGORIZATION	y1	RA-2
RA-3	RISK ASSESSMENT	y1	RA-3
RA-5	VULNERABILITY SCANNING	y1	RA-5
SC-7	BOUNDARY PROTECTION	y1	SC-7
SI-4	INFORMATION SYSTEM MONITORING	y1	SI-4
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	y1	SI-5
AC-6	LEAST PRIVILEGE	y1	AC-6
AT-2	SECURITY AWARENESS TRAINING	y1	AT-2
PE-3	PHYSICAL ACCESS CONTROL	y1	PE-3
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	y1	SC-1
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	y1	SC-8
SC-28	PROTECTION OF INFORMATION AT REST	y1	SC-28
CA-9	INTERNAL SYSTEM CONNECTIONS	y1	CA-9
IR-5	INCIDENT MONITORING	y1	IR-5
MP-6	MEDIA SANITIZATION	y1	MP-6
PE-6	MONITORING PHYSICAL ACCESS	y1	PE-6
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	y1	PL-1
PL-2	SYSTEM SECURITY PLAN	y1	PL-2
PS-2	POSITION RISK DESIGNATION	y1	PS-2
PS-5	PERSONNEL TRANSFER	y1	PS-5
CA-8	PENTRATION TESTING	y1	CA-8
IR-8	INCIDENT RESPONSE PLAN	y2	IR-8
MP-4	MEDIA STORAGE	y2	MP-4

SC-18	MOBILE CODE	y2	SC-18
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	y2	CA-1
CA-2	SECURITY ASSESSMENTS	y2	CA-2
CM-2	BASELINE CONFIGURATION	y2	CM-2
CM-5	ACCESS RESTRICTIONS FOR CHANGE	y2	CM-5
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	y2	CM-8
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	y2	MA-1
PS-3	PERSONNEL SCREENING	y2	PS-3
SA-8	SECURITY ENGINEERING PRINCIPLES	y2	SA-8
AC-4	INFORMATION FLOW ENFORCEMENT	y2	AC-4
IA-11	RE-AUTHENTICATION	y2	IA-11
MP-5	MEDIA TRANSPORT	y2	MP-5
MP-7	MEDIA USE	y2	MP-7
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	y2	PE-2
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	y2	PE-5
CM-7	LEAST FUNCTIONALITY	y2	CM-7
IA-5	AUTHENTICATOR MANAGEMENT	y2	IA-5
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	y2	IA-7
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	y2	IA-8
MA-2	CONTROLLED MAINTENANCE	y2	MA-2
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	y2	AC-19
AC-21	INFORMATION SHARING	y2	AC-21
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	y2	AU-1
AU-8	TIME STAMPS	y2	AU-8
AU-9	PROTECTION OF AUDIT INFORMATION	y2	AU-9
AU-11	AUDIT RECORD RETENTION	y2	AU-11
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	y2	CM-1
CM-3	CONFIGURATION CHANGE CONTROL	y2	CM-3
IA-10	ADAPTIVE IDENTIFICATION AND AUTHENTICATION	y2	IA-10
PE-16	DELIVERY AND REMOVAL	y2	PE-16
PL-8	INFORMATION SECURITY ARCHITECTURE	y2	PL-8
MA-5	MAINTENANCE PERSONNEL	y2	MA-5
AC-5	SEPARATION OF DUTIES	y2	AC-5
AU-2	AUDIT EVENTS	y2	AU-2
AU-3	CONTENT OF AUDIT RECORDS	y2	AU-3
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	y2	AU-6
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	y2	IA-3
IA-6	AUTHENTICATOR FEEDBACK	y2	IA-6
PS-7	THIRD-PARTY PERSONNEL SECURITY	y2	PS-7
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	y2	SA-9
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	y2	SA-10
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	y2	SA-11
SA-12	SUPPLY CHAIN PROTECTION	y2	SA-12
SA-15	DEVELOPMENT PROCESS STANDARDS AND TOOLS	y2	SA-15
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	y2	SA-17
CA-3	SYSTEM INTERCONNECTIONS	y2	CA-3
AU-4	AUDIT STORAGE CAPACITY	y2	AU-4
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	y2	AU-5
AU-12	AUDIT GENERATION	y2	AU-12
CM-4	SECURITY IMPACT ANALYSIS	y2	CM-4

IA-4	IDENTIFIER MANAGEMENT	y2	IA-4
IA-9	SERVICE IDENTIFICATION AND AUTHENTICATION	y2	IA-9
IR-4	INCIDENT HANDLING	y2	IR-4
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	y2	PE-18
PS-8	PERSONNEL SANCTIONS	y3	PS-8
SC-31	COVERT CHANNEL ANALYSIS	y3	SC-31
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	y3	SI-7
CM-11	USER-INSTALLED SOFTWARE	y3	CM-11
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	y3	SA-3
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	y3	AC-20
AU-7	AUDIT REDUCTION AND REPORT GENERATION	y3	AU-7
AU-10	NON_REPUDIATION	y3	AU-10
CA-7	CONTINUOUS MONITORING	y3	CA-7
MA-4	NONLOCAL MAINTENANCE	y3	MA-4
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	y3	PE-4
PS-6	ACCESS AGREEMENTS	y3	PS-6
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	y3	SA-1
SA-4	ACQUISITION PROCESS	y3	SA-4
SA-5	INFORMATION SYSTEM DOCUMENTATION	y3	SA-5
SA-14	CRITICALITY ANALYSIS	y3	SA-14
PM-1	INFORMATION SECURITY PROGRAM PLAN	y3	PM-1
PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	y3	PM-6
PM-14	TESTING, TRAINING, AND MONITORING	y3	PM-14
PM-16	THREAT AWARENESS PROGRAM	y3	PM-16
CM-6	CONFIGURATION SETTINGS	y3	CM-6
CM-9	CONFIGURATION MANAGEMENT PLAN	y3	CM-9
CM-10	SOFTWARE USAGE RESTRICTIONS	y3	CM-10
MA-3	MAINTENANCE TOOLS	y3	MA-3
PE-20	ASSET MANAGEMENT AND TRACKING	y3	PE-20
PM-13	INFORMATION SECURITY WORKFORCE	y3	PM-13
PM-15	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	y3	PM-15
IR-3	INCIDENT RESPONSE TESTING	y3	IR-3
PE-19	INFORMATION LEAKAGE	y3	PE-19
PM-9	RISK MANAGEMENT STRATEGY	y3	PM-9
PM-4	PLAN OF ACTION AND MILESTONES PROCESS	y3	PM-4
PM-8	CRITICAL INFRASTRUCTURE PLAN	y3	PM-8
PM-12	INSIDER THREAT PROGRAM	y3	PM-12
AC-16	SECURITY ATTRIBUTES	y3	AC-16
PM-11	MISSION/BUSINESS PROCESS DEFINITION	y3	PM-11
CP-9	INFORMATION SYSTEM BACKUP	y3	CP-9
SC-44	DETONATION CHAMBERS	y3	SC-44
SC-5	DENIAL OF SERVICE PROTECTION	y3	SC-5
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	y3	CP-1
CP-2	CONTINGENCY PLAN	y3	CP-2
CP-3	CONTINGENCY TRAINING	y3	CP-3
CP-4	CONTINGENCY PLAN TESTING	y3	CP-4
CP-6	ALTERNATE STORAGE SITE	y3	CP-6
CP-8	TELECOMMUNICATIONS SERVICES	y3	CP-8
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	y3	CP-10
CP-11	ALTERNATE COMMUNCATIONS PROTOCOLS	y3	CP-11

PE-9	POWER EQUIPMENT AND CABLING	y3	PE-9
PE-10	EMERGENCY SHUTOFF	y3	PE-10
PE-11	EMERGENCY POWER	y3	PE-11
PE-12	EMERGENCY LIGHTING	y3	PE-12
PE-13	FIRE PROTECTION	y3	PE-13
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	y3	PE-14
PE-15	WATER DAMAGE PROTECTION	y3	PE-15
SC-2	APPLICATION PARTITIONING	y3	SC-2 (added)