Control Parameters for
Cyber Security Fuel Cycle Facility Rulemaking

Notes:

(1) Do not use this table without consulting the regulatory guide for specific guidance.

(2) These controls reference controls from NIST SP 800-53, Revision 4.

PROGRAM MANAGEMENT

Selected Program Management (PM) controls to be deployed organization-wide in support of the information security program. These controls are not associated with specific security control sets.

CNTL NO.	Control Name Control Enhancement Name	Parameters
PM-1	Information Security Program Plan	P1: At least yearly
PM-2	Senior Information Security Officer	-
PM-4	Plan of Action and Milestones Process	-
PM-6	Information Security Measures of Performance	-
PM-9	Risk Management Strategy	P1: At least yearly
PM-10	Security Authorization Process	-
PM-12	Insider Threat Program	-
PM-13	Information Security Workforce	-
PM-14	Testing, Training, and Monitoring	-
PM-15	Contacts with Security Groups and Associations	-
PM-16	Threat Awareness Program	-

ACCESS CONTROL

CNTL NO.	Control Name Control Enhancement Name	Parameters
	ACCESS CONTROL	
AC-1	Access Control Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
AC-2	Account Management	P1: (licensee-defined) P2: (licensee-defined) P3: (licensee-defined) P4: at least every 90 days
AC-3	Access Enforcement	-
AC-8	System Use Notification	P1: (licensee-defined) P2: (licensee-defined)
	AWARENESS AND TRAINING CONTROLS	
AT-1	Security Awareness and Training Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
AT-2	Security Awareness Training	P1: at least yearly
AT-4	Security Training Records	P1: at least 5 years
	AUDIT AND ACCOUNTABILITY CONTROLS	
AU-1	Audit and Accountability Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
	CONFIGURATION MANAGEMENT CONTROLS	
CM-1	Configuration Management Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
CM-3	Configuration Change Control	P1: at least 2 years P2: (licensee-defined) P3: (licensee-defined)
CM-4	Security Impact Analysis	-

CNTL NO.	Control Name Control Enhancement Name	Parameters
CM-5	Access Restrictions for Change	-
CM-8	Information System Component Inventory	P1: (licensee-defined) P2: (licensee-defined) P3: (licensee-defined)
IDENTIFICATION AND AUTHENTICATION CONTROLS		
IA-1	Identification and Authentication Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
IA-2	Identification and Authentication (Organizational Users)	-
INCIDENT RESPONSE CONTROLS		
IR-1	Incident Response Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
IR-2	Incident Response Training	P1: 90 days P2: at least yearly
IR-4	Incident Handling	-
IR-5	Incident Monitoring	-
IR-6	Incident Reporting	P1: (licensee-defined, not to exceed 24 hours) P2: (licensee-defined)
IR-8	Incident Response Plan	P1: (licensee-defined) P2: (licensee-defined) P3: at least yearly P4: (licensee-defined)
INCIDENT RESPONSE CONTROLS		
MA-1	System Maintenance Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
MAINTENANCE CONTROLS		

CNTL NO.	Control Name Control Enhancement Name	Parameters
MP-1	Media Protection Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
MP-2	Media Access	P1: (licensee-defined) P2: (licensee-defined)
SYSTEM AND SERVICES ACQUISITION CONTROLS		
SA-1	System and Services Acquisition Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
SYSTEM AND COMMUNICATIONS PROTECTION CONTROLS		
SC-1	System and Communications Protection Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly
SYSTEM AND INFORMATION INTEGRITY CONTROLS		
SI-1	System and Information Integrity Policy and Procedures	P1: all employees and contractors P2: at least yearly P3: at least yearly