NIST SP 800-53 R4 and NIST SP 80-82 R2 Security Controls Merged

Note: This document is for illustrative purposes only. The document is a merge of the full NIST SP 800-53 R4 control text and the NIST SP 800-82 R2 Appendix G ICS Overlay with Supplemental Guidance and Control Enhancements. For the novice to using the NIST and CNSS publications, trying to look at 3 or 4 disassociated documents and understanding how the control, parameter values, guidance and enhancements interact can be confusing. This document is an example of the output expected as a result of completing the DHS Cyber Security Tool (CSET) Security Plan or the DoD eMASS program.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles*****:**
1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
b. Reviews and updates the current:
1. Access control policy ***annually*** and
2. Access control procedures ***annually.***

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems. ICS access by vendors and maintenance staff can occur over a very large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

AC-2 ACCOUNT MANAGEMENT

Control: The organization:
a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: ***organization-defined information system account types***;
b. Assigns account managers for information system accounts;
c. Establishes conditions for group and role membership;
d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e. Requires approvals by ***organization-defined personnel or roles*** for requests to create information system accounts;

f. Creates, enables, modifies, disables, and removes information system accounts in accordance with ***organization-defined procedures or conditions***;
g. Monitors the use of, information system accounts;
h. Notifies account managers:
1. When accounts are no longer required;
2. When users are terminated or transferred; and
3. When individual information system usage or need-to-know changes;
i. Authorizes access to the information system based on:
1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the organization or associated missions/business functions;
j. Reviews accounts for compliance with account management requirements ***annually***; and
k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Control Enhancements:

(1) *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*
The organization employs automated mechanisms to support the management of information system accounts.

(2) *ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*
The information system automatically removes temporary and emergency accounts after *not to exceed 72 hours.*

(3) *ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*
The information system automatically disables inactive accounts after *not to exceed 90 days.*

(4) *ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*
The information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required, *organization-defined personnel*.

Supplemental Guidance: Related controls: AU-2, AU-12.

(5) *ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*
The organization requires that users log out when *organization defined time-period of expected inactivity and/or description of when to log out*.

Supplemental Guidance: Related control: SI-4.

(12) *ACCOUNT MANAGEMENT | USAGE CONDITIONS*
The organization determines *organization-defined circumstances and/or usage conditions* for *organization-defined information system accounts*.

Supplemental Guidance: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

(13) *ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*
The organization conducts *quarterly* reviews of information system accounts (including access authorizations and shared/group account memberships).

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, auditing measures.

Control Enhancement: (1, 3, 4) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (12, 13) No ICS Supplemental Guidance.

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS. Example compensating controls include encapsulation.

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS. Example compensating controls include encapsulation.

AC-4 INFORMATION FLOW ENHANCEMENT

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on ***organization-defined information flow control policies; at levels 3 and above, ICS***

Historian information flow should be unidirectional to a read only Historian in level 4 or 5 with a DMZ between the levels, preferably with a data diode or flip switch to ensure unidirectional flow. Information flow between the HMI and lower levels can be bidirectional, but should be monitored using passive applications.

No ICS Supplemental Guidance.

AC-5 SEPARATION OF DUTIES

Control: The organization:
a. Separates ***organization-defined duties of individuals*;**
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

ICS Supplemental Guidance: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 LEAST PRIVILEGE

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*
The organization explicitly authorizes access to *organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*.

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*
The organization requires that users of information system accounts, or roles, with access to *organization-defined security functions or security-relevant*

***information*, use nonprivileged accounts or roles, when accessing nonsecurity functions.**

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*
The organization authorizes network access to *organization-defined privileged commands* only for *organization-defined compelling operational needs* and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*
The organization limits authorization to privileged accounts on the information system to *organization-defined personnel*.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*
The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*
The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and

prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

ICS Supplemental Guidance: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access and higher privileges include write access).

Control Enhancement: (1) ICS Supplemental Guidance: In situations where the ICS cannot support access control to security functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support access control to nonsecurity functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (3) ICS Supplemental Guidance: In situations where the ICS cannot support network access control to privileged commands, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (5) ICS Supplemental Guidance: In situations where the ICS cannot support access control to privileged accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (9) ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. Example compensating controls include providing an auditing capability on a separate information system.

Control Enhancement: (10) ICS Supplemental Guidance: Example compensating controls include enhanced auditing.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system:
a. ***Enforces a limit of three consecutive invalid login attempts by a user during a 15 minute time period and automatically locks the account/node until released by an administrator***; and
b. Automatically ***locks the account/node until released by an*** *administrator* when the maximum number of unsuccessful attempts is exceeded.

ICS Supplemental Guidance: Many ICS must remain continuously on and operators remain logged onto the system at all times. A “log-over” capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:
a. Displays to users ***organization-defined system use notification message or banner*** before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
1. Users are accessing a U.S. Government information system;
2. Information system usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
4. Use of the information system indicates consent to monitoring and recording;
b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
c. For publicly accessible systems:
1. Displays system use information ***organization-defined conditions***, before granting further access;
2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Includes a description of the authorized uses of the system.

ICS Supplemental Guidance: Many ICS must remain continuously on and system use notification may not be supported or effective. Example compensating controls include posting physical notices in ICS facilities.

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for ***three (3) sessions for privileged access*** and to ***two (2) sessions for non-privileged access***.

ICS Supplemental Guidance: The number, account type, and privileges of concurrent sessions takes into account the roles and responsibilities of the affected individuals. Example compensating controls include providing increased auditing measures.

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after ***not to exceed 30 minutes, except to fulfill documented, AO approved and validated mission requirement,*** of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Control Enhancements:

(1) *SESSION LOCK | PATTERN-HIDING DISPLAYS*
The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

ICS Supplemental Guidance: This control assumes a staffed environment where users interact with information system displays. When this assumption does not apply the organization tailors the control appropriately (e.g., the ICS may be physically protected by placement in a locked enclosure). The control may also be tailored for ICS that are not configured with displays, but which have the capability to support displays (e.g., ICS to which a maintenance technician may attach a display). In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

Control Enhancement: (1) ICS Supplemental Guidance: ICS may employ physical protection to prevent access to a display or to prevent attachment of a display. In situations where the ICS cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a user session after ***not to exceed 30 minutes, except to fulfill documented, AO approved and validated mission requirement.***

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

a. Identifies ***organization-defined user actions*** that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

No ICS Supplemental Guidance.

AC-17 REMOTE ACCESS

Control: The organization:
a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b. Authorizes remote access to the information system prior to allowing such connections.

Control Enhancements:

(1) *REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*
The information system monitors and controls remote access methods.
Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12.

(2) *REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*
The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13.

(3) *REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*
The information system routes all remote accesses through *organization-defined number* managed network access control points.
Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7.

(4) *REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*
The organization:
(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for *organization-defined needs*; and

(b) Documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Related control: AC-6.

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2], dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity.

Control Enhancement: (2) ICS Supplemental Guidance: ICS security objectives often rank confidentiality below availability and integrity. The organization explores all possible cryptographic mechanism (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. Example compensating controls include providing increased auditing for remote sessions or limiting remote access privileges to key personnel).

Control Enhancement: (3) ICS Supplemental Guidance: Example compensating controls include connection-specific manual authentication of the remote entity.

Control Enhancement: (4) No ICS Supplemental Guidance.

ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-18 WIRELESS ACCESS

Control: The organization:
a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access to the information system prior to allowing such connections.

Control Enhancements:

(1) *WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*
The information system protects wireless access to the system using authentication of *users, devices,* and encryption.

Supplemental Guidance: Related controls: SC-8, SC-13.

(4) *WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*
The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15.

(5) *WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*
The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) ICS Supplemental Guidance: See AC-17 Control Enhancement: (1) ICS Supplemental Guidance. Example compensating controls include providing increased auditing for wireless access or limiting wireless access privileges to key personnel.

Control Enhancement: (4) ICS Supplemental Guidance: Example compensating controls include TBD

Control Enhancement: (5) No ICS Supplemental Guidance.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

Control Enhancements:

(5) *ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*
The organization employs *full-device encryption if possible, otherwise container encryption if possible* to protect the confidentiality and integrity of information on *organization-defined mobile devices to include ICS technicians and operator's mobile diagnostics and calibration devices*.

Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.

No ICS Supplemental Guidance.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:
a. Access the information system from external information systems; and
b. Process, store, or transmit organization-controlled information using external information systems.

Control Enhancements:

(1) *USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:
(a) Verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
(b) Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

Supplemental Guidance: This control enhancement recognizes that there are circumstances where individuals using external information systems (e.g., contractors, coalition partners) need to access organizational information systems. In those situations, organizations need confidence that the external information systems contain the necessary security safeguards (i.e., security controls), so as not to compromise, damage, or otherwise harm organizational information systems. Verification that the required security controls have been implemented can be achieved, for example, by

third-party, independent assessments, attestations, or other means, depending on the confidence level required by organizations. Related control: CA-2.

(2) *USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*
The organization *restricts* the use of organization-controlled portable storage devices by authorized individuals on external information systems.

Supplemental Guidance: Limits on the use of organization-controlled portable storage devices in external information systems include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

ICS Supplemental Guidance: Organizations refine the definition of "external" to reflect lines of authority and responsibility; granularity of organization entity; and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, comes under different managers, or does not provide sufficient visibility into the implementation of security controls to allow the establishment of a satisfactory trust relationship. For example, a process control system and a business data processing system would typically be considered external to each other. Access to an ICS for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external information systems is reexamined with respect to ICS functions, purposes, technology, and limitations to establish a clear documented technical or business case for use and an acceptance of the risk inherent in the use of an external information system.

Control Enhancement: (1, 2) No ICS Supplemental Guidance.

AC-21 INFORMATION SHARING

Control: The organization:
a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for ***organization-defined information sharing circumstances where user discretion is required to include ICS system alerts and advisories with DHS ICS-CERT*** and
b. Employs ***automated vulnerability and patch notification, manual install of patches*** to assist users in making information sharing/collaboration decisions.

ICS Supplemental Guidance: The organization should collaborate and share information about potential incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) http://ics-cert.us-cert.gov/ics-cert/ collaborates with international and

private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. Organizations should consider having both an unclassified and classified information sharing capability.

Rationale for adding AC-21 to low baseline: ICS systems provide essential services and control functions and are often connected to other ICS systems or business systems that can be vectors of attack. It is therefore necessary to provide a uniform defense encompassing all baselines.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:
a. Designates individuals authorized to post information onto a publicly accessible information system;
b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d. Reviews the content on the publicly accessible information system for nonpublic information ***quarterly or as new information is posted*** and removes such information, if discovered.

ICS Supplemental Guidance: Generally, public access to ICS systems is not permitted. Selected information may be transferred to a publicly accessible information system, possibly with added controls (e.g., introduction of fuzziness or delay).

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***
1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
b. Reviews and updates the current:
1. Security awareness and training ***policy at least annually if not otherwise defined in formal organizational policy;*** and
2. Security awareness and training ***procedures at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users;
b. When required by information system changes; and
c. ***At least annually*** thereafter.

Control Enhancements:

(2) *SECURITY AWARENESS | INSIDER THREAT*
The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

Control Enhancement: (2) No ICS Supplemental Guidance.

AT-3 SECURITY TRAINING

Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:
a. Before authorizing access to the information system or performing assigned duties;
b. When required by information system changes; and
c. ***At least annually*** thereafter.

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
b. Retains individual training records for at ***least 5 years or 5 years after completion of a specific training program***.

No ICS Supplemental Guidance.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
b. Reviews and updates the current:
1. Audit and accountability policy ***least 5 years or 5 years after completion of a specific training program*** and
2. Audit and accountability procedures ***least 5 years or 5 years after completion of a specific training program***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

AU-2 AUDITABLE EVENTS

Control: The organization:
a. Determines that the information system is capable of auditing the following events***: (a) successful and unsuccessful attempts to access, modify, or delete security objects, (b) successful and unsuccessful logon attempts, (c) privileged activities or other system level access, (d) starting and ending time for user access to the system, (e) concurrent logons from different workstations, (f) successful and unsuccessful accesses to objects, (g) all program initiations, (h) all direct access to the information system;***
b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d. Determines that the following events are to be audited within the information system: ***all organizations must define a list of audited events in the policy for their organization defined in accordance with AU-***1.

Control Enhancements:

(3) *AUDIT EVENTS | REVIEWS AND UPDATES*
The organization reviews and updates the audited events *at least annually*.

Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient.

ICS Supplemental Guidance: The organization may designate ICS events as audit events, requiring that ICS data and/or telemetry be recorded as audit data.

Control Enhancement: (3) No ICS Supplemental Guidance.

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*
The information system generates audit records containing the following additional information: *organization-defined additional, more detailed information*.

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*
The information system provides centralized management and configuration of the content to be captured in audit records generated by *organization-defined information system components*.

Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

ICS Supplemental Guidance: Example compensating controls include providing an auditing capability on a separate information system.

Control Enhancement: (1, 2) No ICS Supplemental Guidance.

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity in accordance with ***organization-defined audit record storage requirements***.

Control Enhancements:

(1) *AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*
The information system off-loads audit records onto a different system or media than the system being audited.

Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Legacy ICS typically are typically configured with remote storage on a separate information system (e.g., the historian accumulates historical operational ICS data and is backed up for storage at a different site). ICS are currently using online backup services and increasingly moving to Cloud based and Virtualized services. Retention of some data (e.g., SCADA telemetry) may be required by regulatory authorities.

Rationale for adding AU-4 (1) to all baselines: Legacy ICS components typically do not have capacity to store or analyze audit data. The retention periods for some data, particularly compliance data, may require large volumes of storage.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:
a. Alerts ***organization-defined personnel or roles*** in the event of an audit processing failure; and
b. Takes the following additional actions: ***organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)***.

Control Enhancements:

(1) *RESPONSE TO AUDIT PROCESSING FAILURES* | *AUDIT STORAGE CAPACITY*
The information system provides a warning to *organization-defined personnel, roles, and/or locations* within *organization-defined time period* when allocated audit record storage volume reaches organi*zation-defined percentage* of repository maximum audit record storage capacity.

Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

(2) *RESPONSE TO AUDIT PROCESSING FAILURES* | *REAL-TIME ALERTS*
The information system provides an alert in *organization-defined real-time period* to *organization-defined personnel, roles, and/or locations* when the following audit failure events occur: *organization-defined audit failure events requiring real-time alerts*.

Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less).

No ICS Supplemental Guidance.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:
a. Reviews and analyzes information system audit ***on at least on a weekly basis*** for indications of ***organization-defined inappropriate or unusual activity*****;** and
b. Reports findings to ***organization-defined personnel or roles***.

Control Enhancements:

(1) *AUDIT REVIEW, ANALYSIS, AND REPORTING* | *PROCESS INTEGRATION*
The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7.

(3) *AUDIT REVIEW, ANALYSIS, AND REPORTING* | *CORRELATE AUDIT REPOSITORIES*

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4.

(5) *AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*
The organization integrates analysis of audit records with analysis of ***vulnerability scanning information; performance data; information system monitoring information; organization-defined data/information collected from other sources*** to further enhance the ability to identify inappropriate or unusual activity.

Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5.

(6) *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*
The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identify for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations.

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include manual mechanisms or procedures.

Control Enhancement: (3, 5, 6) No ICS Supplemental Guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability that:
a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b. Does not alter the original content or time ordering of audit records.

Control Enhancements:

(1) *AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*
The information system provides the capability to process audit records for events of interest based on *organization-defined audit fields within audit records*.

Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. Related controls: AU-2, AU-12.

No ICS Supplemental Guidance.

Control Enhancement: (1) No ICS Supplemental Guidance.

AU-8 TIME STAMPS

Control: The information system:
a. Uses internal system clocks to generate time stamps for audit records; and
b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets ***organization-defined granularity of time measurement***.

Control Enhancements:

(1) *TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*
The information system:
(a) Compares the internal information system clocks *at least every 24 hours* with the ***ICS system time clock*; and**

(b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than *organization-defined time period*.

Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

ICS Supplemental Guidance: Example compensating controls include using a separate information system designated as an authoritative time source.

Control Enhancement: (1) ICS Supplemental Guidance: ICS employ suitable mechanisms (e.g., GPS, IEEE 1588).

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

(2) *PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*
The information system backs up audit records *not less than weekly* onto a physically different system or system component than the system or component being audited.

Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11.

(3) *PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*
The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13.

(4) *PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*
The organization authorizes access to management of audit functionality to only *organization-defined subset of privileged users*.

Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control

enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5.

No ICS Supplemental Guidance.

AU-10 NON-REPUDIATION

Control: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed ***organization-defined actions to be covered by non-repudiation***.

ICS Supplemental Guidance: Example compensating controls include providing non-repudiation on a separate information system.

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for ***a minimum of 5 years for Sensitive Compartmented Information and Sources And Methods Intelligence information; a minimum of 1 year for all other information (Unclassified through Collateral Top Secret)*** to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

No ICS Supplemental Guidance.

AU-12 AUDIT GENERATION

Control: The information system:
a. Provides audit record generation capability for the auditable events defined in AU-2 a. at ***all information system and network components***;
b. Allows ***organization-defined personnel or roles*** to select which auditable events are to be audited by specific components of the information system; and
c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Control Enhancements:

(1) *AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*

The information system compiles audit records from *organization-defined information system components* into a system-wide (logical or physical) audit trail that is time-correlated to within *organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*.

Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records

to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12.

(3) *AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*
The information system provides the capability for *organization-defined individuals or roles* to change the auditing to be performed on *organization-defined information system components* based on *organization-defined selectable event criteria* within *organization-defined time thresholds*.

Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include providing time-correlated audit records on a separate information system.

Control Enhancement: (3) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles*:**
1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
b. Reviews and updates the current:
1. Security assessment and authorization policy ***at least annually if not otherwise defined in formal organizational policy; at least annually if not otherwise defined in formal organizational policy***; and
2. Security assessment and authorization ***procedures at least annually if not otherwise defined in formal organizational policy; at least annually if not otherwise defined in formal organizational policy.***

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CA-2 SECURITY ASSESSMENTS

Control: The organization:
a. Develops a security assessment plan that describes the scope of the assessment including:
1. Security controls and control enhancements under assessment;
2. Assessment procedures to be used to determine security control effectiveness; and
3. Assessment environment, assessment team, and assessment roles and responsibilities;
b. Assesses the security controls in the information system and its environment of operation ***at least annually*** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
c. Produces a security assessment report that documents the results of the assessment; and
d. Provides the results of the security control assessment to ***organization-defined individuals or roles***.

Control Enhancements:

(1) *SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*
The organization employs assessors or assessment teams with *organization-defined level of independence* to conduct security control assessments.

Supplemental Guidance: Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within organizations or can be contracted to public or private sector entities outside of organizations. Authorizing officials determine the required level of independence based on the security categories of information systems and/or the ultimate risk to organizational operations, organizational assets, or individuals. Authorizing officials also determine if the level of assessor independence provides sufficient assurance that the results are sound and can be used to make credible, risk-based decisions. This includes determining whether contracted security assessment services have sufficient independence, for example, when information system owners are not directly involved in contracting processes or cannot unduly influence the impartiality of assessors conducting assessments. In special situations, for example, when organizations that own the information systems are small or organizational structures require that assessments

are conducted by individuals that are in the developmental, operational, or management chain of system owners, independence in assessment processes can be achieved by ensuring that assessment results are carefully reviewed and analyzed by independent teams of experts to validate the completeness, accuracy, integrity, and reliability of the results. Organizations recognize that assessments performed for purposes other than direct support to authorization decisions are, when performed by assessors with sufficient independence, more likely to be useable for such decisions, thereby reducing the need to repeat assessments.

(2) *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*
The organization includes as part of security control assessments, *organization-defined frequency*, *announced, unannounced*, *in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; and organization-defined other forms of security assessment*.

Supplemental Guidance: Organizations can employ information system monitoring, insider threat assessments, malicious user testing, and other forms of testing (e.g., verification and validation) to improve readiness by exercising organizational capabilities and indicating current performance levels as a means of focusing actions to improve security. Organizations conduct assessment activities in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Authorizing officials approve the assessment methods in coordination with the organizational risk executive function. Organizations can incorporate vulnerabilities uncovered during assessments into vulnerability remediation processes. Related controls: PE-3, SI-2.

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that the assessment does not affect system operation or result in intentional or unintentional system modification. If assessment activities must be performed on the production ICS, it may need to be taken off-line before an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible.

Control Enhancement: (1) No ICS Supplemental Guidance.

Control Enhancement: (2) ICS Supplemental Guidance: The organization conducts risk analysis to support the selection of assessment target (e.g., the live system, an off-line replica, a simulation).

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization:
a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c. Reviews and updates Interconnection Security Agreements ***organization-defined frequency***.

Control Enhancements:

(5) *SYSTEM INTERCONNECTIONS* | *RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*
The organization employs *deny-all, permit-by-exception* policy for allowing *organization-defined information systems* to connect to external information systems.

Supplemental Guidance: Organizations can constrain information system connectivity to external domains (e.g., websites) by employing one of two policies with regard to such connectivity: (i) allow-all, deny by exception, also known as *blacklisting* (the weaker of the two policies); or (ii) deny-all, allow by exception, also known as *whitelisting* (the stronger of the two policies). For either policy, organizations determine what exceptions, if any, are acceptable. Related control: CM-7.

ICS Supplemental Guidance: Organizations perform risk-benefit analysis to support determination whether an ICS should be connected to other information system(s). The Authorizing Official fully understands the organizational information security policies and procedures; the ICS security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the connected to other information system(s); and the specific health, safety, and environmental risks associated with a particular interconnection. The AO documents risk acceptance in the ICS system security plan.

Control Enhancement: (5) No ICS Supplemental Guidance.

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization:
a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
b. Updates existing plan of action and ***at least quarterly*** based on the findings from security

No ICS Supplemental Guidance.

CA-6 SECURITY AUTHORIZATION

Control: The organization:
a. Assigns a senior-level executive or manager as the authorizing official for the information system;
b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
c. Updates the security authorization ***at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates***.

No ICS Supplemental Guidance.

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:
a. Establishment of ***organization-defined metrics*** to be monitored;
b. Establishment of ***organization-defined frequencies*** for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of organization and the information system to ***organization-defined personnel or roles*****,** ***organization-defined frequency***.

Control Enhancements:

(1) *CONTINUOUS MONITORING* | *INDEPENDENT ASSESSMENT*

The organization employs assessors or assessment teams with *organization-defined level of independence* to monitor the security controls in the information system on an ongoing basis.

Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence

provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services.

ICS Supplemental Guidance: Continuous monitoring programs for ICS are designed, documented, and implemented by qualified personnel (i.e., experienced with ICS) selected by the organization. The organization ensures that continuous monitoring does not interfere with ICS functions. The individual/group designing and conducting the continuous monitoring fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that continuous monitoring does not affect system operation or result in intentional or unintentional system modification. Example compensating controls include external monitoring.

Control Enhancement: (1) No ICS Supplemental Guidance.

CA-8 PENETRATION TESTING

Control: The organization conducts penetration testing ***organization-defined frequency*** on ***organization-defined information systems or system components*****.**

ICS Supplemental Guidance: Penetration testing is used with care on ICS networks to ensure that ICS functions are not adversely impacted by the testing process. In general, ICS are highly sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Production ICS may need to be taken off-line before testing can be conducted. If ICS are taken off-line for testing, tests are scheduled to occur during planned ICS outages whenever possible. If penetration testing is performed on non-ICS networks, extra care is taken to ensure that tests do not propagate into the ICS network.

CA-9 INTERNAL SYSTEM CONNECTIONS

Control: The organization:
a. Authorizes internal connections of ***organization-defined information system components or classes of components*** to the information system; and
b. Documents, for each internal connection, the interface

ICS Supplemental Guidance: Organizations perform risk-benefit analysis to support determination whether an ICS should be connected to other internal information system(s) and (separate) constituent system components. The Authorizing Official fully understands the organizational information security policies and procedures; the ICS

security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the connected to other information system(s) and (separate) constituent system components, whether by authorizing each individual internal connection or authorizing internal connections for a class of components with common characteristics and/or configurations; and the specific health, safety, and environmental risks associated with a particular interconnection. The AO documents risk acceptance in the ICS system security plan.

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
b. Reviews and updates the current:
1. Configuration management policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. Configuration management procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Control Enhancements:

(1) *BASELINE CONFIGURATION | REVIEWS AND UPDATES*
The organization reviews and updates the baseline configuration of the information system:
(a) *At least annually*;
(b) When required due to *significant or security relevant changes, or security incidents*; and
(c) As an integral part of information system component installations and upgrades.

Supplemental Guidance: Related control: CM-5.

(2) *BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5.

(3) *BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*

The organization retains *at least two prior versions* to support rollback.

Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records.

(7) *BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*

The organization:
(a) Issues *organization-defined information systems, system components, or devices* with *organization-defined configurations* to individuals traveling to locations that the organization deems to be of significant risk; and
(b) Applies *organization-defined security safeguards* to the devices when the individuals return.

No ICS Supplemental Guidance.

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:
a. Determines the types of changes to the information system that are configuration-controlled;
b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
c. Documents configuration change decisions associated with the information system;

d. Implements approved configuration-controlled changes to the information system;
e. Retains records of configuration-controlled changes to the information system for ***at least 90 days***;
f. Audits and reviews activities associated with configuration-controlled changes to the information system; and
g. Coordinates and provides oversight for configuration change control activities through ***organization-defined configuration change control element (e.g., committee, board***) that convenes ***organization-defined frequency***; ***organization-defined configuration change conditions***.

Control Enhancements:

(1) *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*
The organization employs automated mechanisms to:
(a) Document proposed changes to the information system;
(b) Notify *organizational-defined approval authorities* of proposed changes to the information system and request change approval;
(c) Highlight proposed changes to the information system that have not been approved or disapproved by *organization-defined time period*;
(d) Prohibit changes to the information system until designated approvals are received;
(e) Document all changes to the information system; and
(f) Notify *organization-defined personnel* when approved changes to the information system are completed.

(2) *CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*
The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems).

No ICS Supplemental Guidance.

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Control Enhancements:

(1) *SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*
The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7.

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

Control Enhancement: (1) No ICS Supplemental Guidance.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Control Enhancements:

(1) *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*
The information system enforces access restrictions and supports auditing of the enforcement actions.

Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) *ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*

The organization reviews information system changes *at least annually* and *organization-defined circumstances* to determine whether unauthorized changes have occurred.

Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) *ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*
The information system prevents the installation of *organization-defined software and firmware components* without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7.

No ICS Supplemental Guidance.

CM-6 CONFIGURATION SETTINGS

Control: The organization:
a. Establishes and documents configuration settings for information technology products employed within the information system using ***organization-defined security configuration checklists*** that reflect the most restrictive mode consistent with operational requirements;
b. Implements the configuration settings;
c. Identifies, documents, and approves any deviations from established configuration settings for ***organization-defined information system components*** based on ***organization-defined operational requirements***; and
d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.
Control Enhancements:

(1) *CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*
The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for *organization-defined information system components*.

Supplemental Guidance: Related controls: CA-7, CM-4.

(2) *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*

The organization employs *organization-defined security safeguards* to respond to unauthorized changes to *organization-defined configuration settings*.

Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7.

No ICS Supplemental Guidance.

CM-7 LEAST FUNCTIONALITY

Control: The organization:
a. Configures the information system to provide only essential capabilities; and
b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: ***organization-defined prohibited or restricted functions, ports, protocols, and/or services***.

Control Enhancements:

(1) *LEAST FUNCTIONALITY | PERIODIC REVIEW*
The organization:
(a) Reviews the information system *at least annually* to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
(b) Disables *organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure*.

Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2.

(2) *LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*
The information system prevents program execution in accordance with*: organization-defined policies regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage*.

Supplemental Guidance: Related controls: CM-8, PM-5.

(4) *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*
The organization:
(a) Identifies *organization-defined software programs not authorized to execute on the information system*;
(b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

(c) Reviews and updates the list of unauthorized software programs *organization-defined frequency*.

Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as *blacklisting*. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5.

(5) *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*
The organization:
(a) Identifies *organization-defined software programs authorized to execute on the information system*;
(b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
(c) Reviews and updates the list of authorized software programs *organization-defined frequency*.

Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as *whitelisting*. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (1, 2, 5) No ICS Supplemental Guidance.

Control Baseline Supplement Rationale: (1) Periodic review and removal of unnecessary and/or nonsecure functions, ports, protocols, and services are added to the LOW baseline because many of the LOW impact ICS components could adversely effect the systems to which they are connected.

(4, 5) Whitelisting (CE 5) is more effective than blacklisting (CE 4). The set of applications that run in ICS is essentially static, making whitelisting practical. ICS-CERT recommends deploying application whitelisting on ICS. Reference: http://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization:
a. Develops and documents an inventory of information system components that:
1. Accurately reflects the current information system;

2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes ***hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name***; and
b. Reviews and updates the information system component inventory ***organization-defined frequency***.

Control Enhancements:

(1) *INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*
The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Supplemental Guidance: Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related control: SI-7.

(3) *INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*
The organization:
(a) Employs automated mechanisms *organization-defined frequency* to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
(b) Takes the following actions when unauthorized components are detected: *disables network access by such components; isolates the components; notifies organization-defined personnel or roles*.

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be

implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing. Related controls: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(4) *INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*
The organization includes in the information system component inventory information, a means for identifying by *position or role*, individuals responsible/accountable for administering those components.
Supplemental Guidance: Identifying individuals who are both responsible and accountable for administering information system components helps to ensure that the assigned components are properly administered and organizations can contact those individuals if some action is required (e.g., component is determined to be the source of a breach/compromise, component needs to be recalled/replaced, or component needs to be relocated).

(5) *INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*
The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Supplemental Guidance: This control enhancement addresses the potential problem of duplicate accounting of information system components in large or complex interconnected systems.

No ICS Supplemental Guidance.

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information system that:
a. Addresses roles, responsibilities, and configuration management processes and procedures;
b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c. Defines the configuration items for the information system and places the configuration items under configuration management; and
d. Protects the configuration management plan from unauthorized disclosure and modification.

No ICS Supplemental Guidance.

CM-10 SOFTWARE USAGE RESTRICTIONS

Control: The organization:
a. Uses software and associated documentation in accordance with contract agreements and copyright laws;
b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

No ICS Supplemental Guidance.

CM-11 USER-INSTALLED SOFTWARE

Control: The organization:
a. Establishes ***organization-defined policies*** governing the installation of software by users;
b. Enforces software installation policies through ***organization-defined methods***; and
c. Monitors policy compliance at ***organization-defined frequency***.

No ICS Supplemental Guidance.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
b. Reviews and updates the current:
1. Contingency planning policy ***at least annually if not otherwise defined in formal organizational policy*** and
2. Contingency planning procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CP-2 CONTINGENCY PLAN

Control: The organization:
a. Develops a contingency plan for the information system that:
1. Identifies essential missions and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;
3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
6. Is reviewed and approved by ***organization-defined personnel or roles***;
b. Distributes copies of the contingency plan to ***key personnel and organizational elements identified in the contingency plan***;
c. Coordinates contingency planning activities with incident handling activities;
d. Reviews the contingency plan for the information system ***at least annually***;
e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicates contingency plan changes to ***key personnel and organizational elements identified in the contingency plan***; and
g. Protects the contingency plan from unauthorized disclosure and modification.

Control Enhancements:

(1) *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*
The organization coordinates contingency plan development with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans.

(2) *CONTINGENCY PLAN | CAPACITY PLANNING*
The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning.

(3) *CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of essential missions and business functions within *12 hours or as defined in the contingency plan* of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(4) *CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the resumption of all missions and business functions within *5 mission/business days or as defined in the contingency plan* of contingency plan activation.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12.

(5) *CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12.

(8) *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*
The organization identifies critical information system assets supporting essential missions and business functions.

Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses.

Organizations identify critical information system assets so that additional safeguards and countermeasures can be employed (above and beyond those safeguards and countermeasures routinely implemented) to help ensure that organizational missions/business functions can continue to be conducted during contingency operations. In addition, the identification of critical information assets facilitates the prioritization of organizational resources. Critical information system assets include technical and operational aspects. Technical aspects include, for example, information technology services, information system components, information technology products, and mechanisms. Operational aspects include, for example, procedures (manually executed operations) and personnel (individuals operating technical safeguards and/or executing manual procedures). Organizational program protection plans can provide assistance in identifying critical assets. Related controls: SA-14, SA-15.

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure).

Control Enhancement: (1) ICS Supplemental Guidance: Organizational elements responsible for related plans may include suppliers such as electric power, fuel, fresh water and wastewater.

Control Enhancement: (2) No ICS Supplemental Guidance.

Control Enhancement: (3, 4) ICS Supplemental Guidance: Plans for the resumption of essential missions and business functions, and for resumption of all missions and business functions take into account the effects of the disruption on the environment of operation. Restoration and resumption plans should include prioritization of efforts. Disruptions may affect the quality and quantity of resources in the environment, such as electric power, fuel, fresh water and wastewater, and the ability of these suppliers to also resume provision of essential mission and business functions. Contingency plans for widespread disruption may involve specialized organizations (e.g., FEMA, emergency services, regulatory authorities). Reference: NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.

CP-3 CONTINGENCY TRAINING

Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities:
a. Within ***organization-defined time period*** of assuming a contingency role or responsibility;
b. When required by information system changes; and
c. ***At least annually or as defined in the contingency plan*** thereafter.

Control Enhancements:

(1) *CONTINGENCY TRAINING* | *SIMULATED EVENTS*
The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

No ICS Supplemental Guidance.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:
a. Tests the contingency plan for the information system ***at least annually or as defined in the contingency plan*** using ***organization-defined tests*** to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b. Reviews the contingency plan test results; and
c. Initiates corrective actions, if needed.

Control Enhancements:

(1) *CONTINGENCY PLAN TESTING* | *COORDINATE WITH RELATED PLANS*
The organization coordinates contingency plan testing with organizational elements responsible for related plans.

Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8.

(2) *CONTINGENCY PLAN TESTING* | *ALTERNATE PROCESSING SITE*
The organization tests the contingency plan at the alternate processing site:
(a) To familiarize contingency personnel with the facility and available resources; and
(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Supplemental Guidance: Related control: CP-7.

No ICS Supplemental Guidance.

CP-6 ALTERNATE STORAGE SITE

Control: The organization:

a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Control Enhancements:

(1) *ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*
The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) *ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*
The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) *ALTERNATE STORAGE SITE | ACCESSIBILITY*

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.

No ICS Supplemental Guidance.

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:
a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of ***organization-defined information system operations*** for essential missions/business functions within ***not to exceed 12 hours*** when the primary processing capabilities are unavailable;

b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

Control Enhancements:

(1) *ALTERNATE PROCESSING SITE* | *SEPARATION FROM PRIMARY SITE*
The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

(2) *ALTERNATE PROCESSING SITE* | *ACCESSIBILITY*
The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3.

(3) *ALTERNATE PROCESSING SITE* | *PRIORITY OF SERVICE*
The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site.

(4) *ALTERNATE PROCESSING SITE* | *PREPARATION FOR USE*
The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6.

No ICS Supplemental Guidance.

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of ***organization-defined information system operations*** for essential missions and business functions within ***not to exceed 12 hours*** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Control Enhancements:

(1) *TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*
The organization:
(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions.

(2) *TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*
The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*
The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission.

Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment.

(4) *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*
The organization:
(a) Requires primary and alternate telecommunications service providers to have contingency plans;
(b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
(c) Obtains evidence of contingency testing/training by providers *organization-defined frequency*.

Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

ICS Supplemental Guidance: Quality of service factors for ICS include latency and throughput.

Control Enhancement: (1, 2, 3, 4) No ICS Supplemental Guidance.

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:
a. Conducts backups of user-level information contained in the information system ***at least weekly or as defined in the contingency plan;***
b. Conducts backups of system-level information contained in the information system ***at least weekly or as defined in the contingency plan***;
c. Conducts backups of information system documentation including security-related documentation ***when created or received, when updated, or as defined in the contingency plan*** and
d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Control Enhancements:

(1) *INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*

The organization tests backup information *not less than monthly, or as defined in the contingency plan* to verify media reliability and information integrity.

(2) *INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*
The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

Supplemental Guidance: Related control: CP-4.

(3) *INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*
The organization stores backup copies of *organization-defined critical information system software and other security-related information* in a separate facility or in a fire-rated container that is not collocated with the operational system.

Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8.

(5) *INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*
The organization transfers information system backup information to the alternate storage site *within 12 hours*.

Supplemental Guidance: Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media.

No ICS Supplemental Guidance.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

(2) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*
The information system implements transaction recovery for systems that are transaction-based.

Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling.

(4) *INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*

The organization provides the capability to restore information system components within *12 hours* from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2.

ICS Supplemental Guidance: Reconstitution of the ICS includes consideration whether system state variables should be restored to initial values or values before disruption (e.g., are valves restored to full open, full closed, or settings prior to disruption). Restoring system state variables may be disruptive to ongoing physical processes (e.g., valves initially closed may adversely affect system cooling).

Control Enhancement: (2, 3, 4, 5) No ICS Supplemental Guidance.

CP-12 SAFE MODE

Control: The information system, when ***organization-defined conditions*** are detected, enters a safe mode of operation with ***organization-defined restrictions of safe mode of operation***.

ICS Supplemental Guidance: The organization-defined conditions and corresponding restrictions of safe mode of operation may vary among baselines. The same condition(s) may trigger different response depending on the impact level. The conditions may be external to the ICS (e.g., electricity supply brown-out). Related controls: SI-17.

Rationale for adding CP-12 to all baselines: This control provides a framework for the organization to plan their policy and procedures for dealing with conditions beyond their control in the environment of operations. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:

1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:
1. Identification and authentication policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. Identification and authentication procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*
The information system implements multifactor authentication for network access to privileged accounts.

Supplemental Guidance: Related control: AC-6.

(2) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*
The information system implements multifactor authentication for network access to non-privileged accounts.

(3) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*
The information system implements multifactor authentication for local access to privileged accounts.

Supplemental Guidance: Related control: AC-6.
(4) *IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*
The information system implements multifactor authentication for local access to non-privileged accounts.

(8) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*
The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages.

Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(9) *IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*
The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

(11) *IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*
The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets *organization-defined strength of mechanism requirements*.

Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor authentication is to reduce the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on organizational information systems can potentially compromise such credentials resident on the system and subsequently impersonate authorized users. Related control: AC-6.

(12) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*
The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Supplemental Guidance: This control enhancement applies to organizations implementing logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is

critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. Example compensating controls include providing increased physical security, personnel security, and auditing measures. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access. See AC-17 ICS Supplemental Guidance. Local user access to ICS components is enabled only when necessary, approved, and authenticated.

Control Enhancement: (1, 2, 3, 4) ICS Supplemental Guidance: Example compensating controls include implementing physical security measures.

Control Enhancement: (8, 9) ICS Supplemental Guidance: Example compensating controls include provide replay-resistance in an external system.

Control Enhancement: (11) No ICS Supplemental Guidance.

Control Enhancement: (12) ICS Supplemental Guidance: Example compensating controls include implementing support for PIV external to the ICS.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates ***all network connected endpoint devices*** before establishing a ***network*** connection.

Control Enhancements:
(1) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*
The information system authenticates *all network connected endpoint devices* before establishing *network* connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13.

(4) *DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*
The organization ensures that device identification and authentication based on attestation is handled by *organization-defined configuration management process*.

Supplemental Guidance: Device attestation refers to the identification and authentication of a device based on its configuration and known operating state. This might be determined via some cryptographic hash of the device. If device attestation is the means of identification and authentication, then it is important that patches and updates to the device are handled via a configuration management process such that the those patches/updates are done securely and at the same time do not disrupt the identification and authentication to other devices.

ICS Supplemental Guidance: The organization may permit connection of devices, also known as non-person entities (NPE), belonging to and authorized by another organization (e.g., business partners) to their ICS. Especially when these devices are non-local, their identification and authentication can be vital. Organizations may perform risk and impact analysis to determine the required strength of authentication mechanisms. Example compensating controls include implementing physical security measures.

Control Enhancement: (1, 4) ICS Supplemental Guidance: Configuration management for NPE identification and authentication customarily involves a human surrogate or representative for the NPE. Devices are provided with their identification and authentication credentials based on assertions by the human surrogate. The human surrogate also responds to events and anomalies (e.g., credential expiration). Credentials for software entities (e.g., autonomous processes not associated with a specific person) based on properties of that software (e.g., digital signatures) may change every time the software is changed or patched. Special purpose hardware (e.g., custom integrated circuits and printed-circuit boards) may exhibit similar dependencies. Organization definition of parameters may be different among the impact levels.

Rationale (applies to control and control enhancements): ICS may exchange information with many external systems and devices. Identifying and authenticating the devices introduces situations that do not exist with humans. These controls include assignments that enable the organization to specifically enumerated that are selected; or to categorize devices by types, models, or other group characteristics. Assignments also enable the organizations to select appropriate controls for local, remote, and network connections.

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers by:
a. Receiving authorization from ***organization-defined personnel or roles*** to assign an individual, group, role, or device identifier;
b. Selecting an identifier that identifies an individual, group, role, or device;
c. Assigning the identifier to the intended individual, group, role, or device;
d. Preventing reuse of identifiers for ***at least one year***; and
e. Disabling the identifier after ***not to exceed 35 days***.

No ICS Supplemental Guidance.

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
b. Establishing initial authenticator content for authenticators defined by the organization;
c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e. Changing default content of authenticators prior to information system installation;
f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
g. Changing/refreshing authenticators ***not to exceed 180 days for passwords***;
h. Protecting authenticator content from unauthorized disclosure and modification;
i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
j. Changing authenticators for group/role accounts when membership to those accounts changes.

Control Enhancements:
(1) *AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*
The information system, for password-based authentication:
(a) Enforces minimum password complexity of *a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each*;
(b) Enforces at least the following number of changed characters when new passwords are created: *at least four*;
(c) Stores and transmits only encrypted representations of passwords;
(d) Enforces password minimum and maximum lifetime restrictions of *24 hours minimum and 180 days maximum*;
(e) Prohibits password reuse for *a minimum of 10* generations; and
(f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does *not* apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity the requirements in the enhancement. Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in

the current password. Password lifetime restrictions do not apply to temporary passwords. Related control: IA-6.

(2) *AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*
The information system, for PKI-based authentication:
(a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
(b) Enforces authorized access to the corresponding private key;
(c) Maps the authenticated identity to the account of the individual or group; and
(d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6.

(3) *AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*
The organization requires that the registration process to receive *organization-defined types of and/or specific authenticators* be conducted *in person; by a trusted third party* before *organization-defined registration authority* with authorization by *organization-defined personnel or roles*.

(11) *AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*
The information system, for hardware token-based authentication, employs mechanisms that satisfy *organization-defined token quality requirements*.

Supplemental Guidance: Hardware token-based authentication typically refers to the use of PKI-based tokens, such as the U.S. Government Personal Identity Verification (PIV) card. Organizations define specific requirements for tokens, such as working with a particular PKI.

ICS Supplemental Guidance: Example compensating controls include physical access control, encapsulating the ICS to provide authentication external to the ICS.

Control Enhancement: (1, 2, 3, 11) No ICS Supplemental Guidance.

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

ICS Supplemental Guidance: This control assumes a visual interface that provides feedback of authentication information during the authentication process. When ICS authentication uses an interface that does not support visual feedback, (e.g., protocol-based authentication) this control may be tailored out.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

No ICS Supplemental Guidance.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Enhancements:

(1) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*
The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4.

(2) *IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*
The information system accepts only FICAM-approved third-party credentials.
Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2.

(3) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS*

The organization employs only FICAM-approved information system components in *organization-defined information systems* to accept third-party credentials.

Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4.

(4) *IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES*

The information system conforms to FICAM-issued profiles.

ICS Supplemental Guidance: The ICS Supplemental Guidance for IA-2, Identification and Authentication (Organizational Users), is applicable for Non- Organizational Users.

Control Enhancement: (1, 2, 3, 4) ICS Supplemental Guidance: Example compensating controls include implementing support external to the ICS and multi-factor authentication.

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

1. Incident response ***policy at least annually if not otherwise defined in formal organizational policy***; and

2. Incident response procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

a. Within ***at least annually*** of assuming an incident response role or responsibility;

b. When required by information system changes; and
c. ***At least annually*** thereafter.

Control Enhancements:

(1) *INCIDENT RESPONSE TRAINING* | *SIMULATED EVENTS*
The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) *INCIDENT RESPONSE TRAINING* | *AUTOMATED TRAINING ENVIRONMENTS*
The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

No ICS Supplemental Guidance.

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system ***at least annually*** using ***organization-defined tests*** to determine the incident response effectiveness and documents the results.

Control Enhancements:

(2) *INCIDENT RESPONSE TESTING* | *COORDINATION WITH RELATED PLANS*
The organization coordinates incident response testing with organizational elements responsible for related plans.

Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

No ICS Supplemental Guidance.

IR-4 INCIDENT HANDLING

Control: The organization:
a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Control Enhancements:

(1) *INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*
The organization employs automated mechanisms to support the incident handling process.

Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems.

(4) *INCIDENT HANDLING | INFORMATION CORRELATION*
The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations.

No ICS Supplemental Guidance.

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Control Enhancements:

(1) *INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*
The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.

No ICS Supplemental Guidance.

IR-6 INCIDENT REPORTING

Control: The organization:
a. Requires personnel to report suspected security incidents to the organizational incident response capability within ***organization-defined time period***; and
b. Reports security incident information to ***organization-defined authorities, but a minimum to DHS ICS-CERT***.

Control Enhancements:

(1) *INCIDENT REPORTING | AUTOMATED REPORTING*
The organization employs automated mechanisms to assist in the reporting of security incidents.

Supplemental Guidance: Related control: IR-7.

ICS Supplemental Guidance: The organization should report incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) http://ics-cert.us-cert.gov/ics-cert/ collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Control Enhancement: (1) ICS Supplemental Guidance: The automated mechanisms used to support the incident reporting process are not necessarily part of, or connected to, the ICS.

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Control Enhancements:

(1) *INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*
The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

No ICS Supplemental Guidance.

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:
a. Develops an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by ***organization-defined personnel or roles*****;**
b. Distributes copies of the incident response plan to ***all personnel with a role or responsibility for implementing the incident response plan***;
c. Reviews the incident response ***plan at least annually (incorporating lessons learned from past incidents)***;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes ***to all personnel with a role or responsibility for implementing the incident response plan, not later than 30 days after the change is made***; and
f. Protects the incident response plan from unauthorized disclosure and modification.

No ICS Supplemental Guidance.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
b. Reviews and updates the current:
1. System maintenance policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. System maintenance procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

MA-2 CONTROLLED MAINTENANCE

Control: The organization:
a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Requires that ***organization-defined personnel or roles*** explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
f. Includes ***organization-defined maintenance-related information*** **in** organizational maintenance records.

Control Enhancements:

(2) *CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*
The organization:
(a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
(b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.
Supplemental Guidance: Related controls: CA-7, MA-3.

No ICS Supplemental Guidance.

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors information system maintenance tools.

Control Enhancements:

(1) *MAINTENANCE TOOLS | INSPECT TOOLS*
The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.
Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code,

(2) *MAINTENANCE TOOLS | INSPECT MEDIA*

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.
Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3.

(3) *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*
The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:
(a) Verifying that there is no organizational information contained on the equipment;
(b) Sanitizing or destroying the equipment;
(c) Retaining the equipment within the facility; or
(d) Obtaining an exemption from *organization-defined personnel or roles* explicitly authorizing removal of the equipment from the facility.
Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards.

No ICS Supplemental Guidance.

MA-4 NON-LOCAL MAINTENANCE

Control: The organization:
a. Approves and monitors nonlocal maintenance and diagnostic activities;
b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
d. Maintains records for nonlocal maintenance and diagnostic activities; and
e. Terminates session and network connections when nonlocal maintenance is completed.

(2) *NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*
The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

(3) *NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*
The organization:
(a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
(b) Removes the component to be serviced from the information system and prior to nonlocal maintenance or diagnostic services, sanitizes the component (with

regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

Supplemental Guidance: Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7.

No ICS Supplemental Guidance.

Control Enhancement: (2) No ICS Supplemental Guidance.

Control Enhancement: (3) ICS Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to non local maintenance and diagnostic services in order to restore essential ICS operations or services. Example compensating controls include limiting the extent of the maintenance and diagnostic services to the minimum essential activities, carefully monitoring and auditing the non-local maintenance and diagnostic activities.

MA-5 MAINTENANCE PERSONNEL

Control: The organization:
a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Control Enhancements:

(1) *MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*
The organization:
(a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
(1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
(b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2.

No ICS Supplemental Guidance.

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and/or spare parts for ***organization-defined information system components***, within ***organization-defined time period*** of failure, ***typically within 24 hours for Low and Moderate Availability or immediately for High Availability***.

No ICS Supplemental Guidance.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates the current:
1. Media protection policy ***at least annually if not otherwise defined in formal organizational policy*** and
2. Media protection procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

MP-2 MEDIA ACCESS

Control: The organization restricts access to ***organization-defined types of digital and/or non-digital media*** to ***organization-defined personnel or roles***.

No ICS Supplemental Guidance.

MP-3 MEDIA MARKING

Control: The organization:
a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts ***organization-defined types of information system media*** from marking as long as the media remain within ***organization-defined controlled areas***.

No ICS Supplemental Guidance.

MP-4 MEDIA STORAGE

Control: The organization:
a. Physically controls and securely stores ***digital and non-digital media containing sensitive, controlled, and/or classified information*** within ***in an area or container approved for processing and storing media based on the sensitivity and/or classification of the information maintained within the media***; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

No ICS Supplemental Guidance.

MP-5 MEDIA TRANSPORT

Control: The organization:
a. Protects and controls ***digital and non-digital media containing sensitive, controlled, and/or classified information*** during transport outside of controlled areas using ***organization-defined security safeguards***;
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Control Enhancements:

(4) *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*
The organization ensures that:
(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and
(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements.

Supplemental Guidance: Related control: PS-3.

No ICS Supplemental Guidance.

MP-6 MEDIA SANITIZATION

Control: The organization:
a. Sanitizes ***organization-defined information system media*** prior to disposal, release out of organizational control, or release for reuse using ***organization-defined sanitization techniques and procedures*** in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Control Enhancements:

(1) *MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Supplemental Guidance: Organizations review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Organizations verify that the sanitization of the media was effective prior to disposal. Related control: SI-12.

(2) *MEDIA SANITIZATION | EQUIPMENT TESTING*
The organization tests sanitization equipment and procedures *at least annually if not otherwise defined in formal organizational policy* to verify that the intended sanitization is being achieved.

Supplemental Guidance: Testing of sanitization equipment and procedures may be conducted by qualified and authorized external entities (e.g., other federal agencies or external service providers).

(3) *MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*
The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: *organization-defined circumstances requiring sanitization of portable storage devices*.

Supplemental Guidance: This control enhancement applies to digital media containing classified information and Controlled Unclassified Information (CUI). Portable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown and potentially untrustworthy sources and may contain malicious code that can be readily transferred to information systems through USB ports or other entry portals. While scanning such storage devices is always recommended, sanitization provides additional assurance that the devices are free of malicious code to include code capable of initiating zero-day attacks. Organizations consider nondestructive sanitization of portable storage devices when such devices are first purchased from the manufacturer or vendor prior to initial use or when organizations lose a positive chain of custody for the devices. Related control: SI-3.

No ICS Supplemental Guidance.

MP-7 MEDIA STORAGE

Control: The organization ***restricts or prohibits*** the use of ***organization-defined types of information system media*** on ***organization-defined information systems or system components*** using ***organization-defined security safeguards***.

Control Enhancements:

(1) *MEDIA USE | PROHIBIT USE WITHOUT OWNER*
The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.
Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4.

No ICS Supplemental Guidance.

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates the current:
1. Physical and environmental protection policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. Physical and environmental protection procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network ICS. Regulatory controls may also apply.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:
a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals ***at least annually*** and
d. Removes individuals from the facility access list when access is no longer required.

No ICS Supplemental Guidance.

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:
a. Enforces physical access authorizations at ***organization-defined entry/exit points to the facility where the information system resides*** by;
1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress/egress to the facility using ***organization-defined physical access control systems/devices*** **or** ***guards***;
b. Maintains physical access audit logs for ***organization-defined entry/exit points***;
c. Provides ***organization-defined security safeguards*** to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity ***organization-defined circumstances requiring visitor escorts and monitoring***;
e. Secures keys, combinations, and other physical access devices;
f. Inventories ***organization-defined physical access devices*** every ***organization-defined frequency***; and

g. Changes combinations and keys ***organization-defined frequency*** and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Control Enhancements:

(1) *PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*
The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at *organization-defined physical spaces containing one or more components of the information system*.

Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2.

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Control Enhancement: (1) No ICS Supplemental Guidance.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to ***organization-defined information system distribution and transmission lines*** within organizational facilities using ***organization-defined security safeguards***.

No ICS Supplemental Guidance.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

No ICS Supplemental Guidance.

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:
a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access ***logs at least every 90 days if not otherwise defined in formal organizational policy*** and upon occurrence of ***organization-defined events or potential indications of events***; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Control Enhancements:

(1) *MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*
The organization monitors physical intrusion alarms and surveillance equipment.

(4) *MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*
The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as *organization-defined physical spaces containing one or more components of the information system*.

Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.

ICS Supplemental Guidance: Physical access controls and defense-in-depth measures are used as compensating controls by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to monitor, detect and alarm when an ICS has been accessed. These compensating controls are in addition to the PE-6 controls (e.g., employing PE-3(4) Lockable Casings and/or PE-3(5) Tamper Protection).

Control Enhancement: (1) No ICS Supplemental Guidance.
Control Enhancement: (4) ICS Supplemental Guidance: The locations of ICS components (e.g., field devices, remote terminal units) can include various remote locations (e.g., substations, pumping stations).

Rationale (adding CE 4 to MODERATE baseline): Many of the ICS components are in remote geographical and dispersed locations with little capability to monitor all ICS components. Other components may be in ceilings, floors, or distribution closets with minimal physical barriers to detect, delay or deny access to the devices and no electronic surveillance or guard forces response capability.

PE-7 VISITOR CONTROL

[Withdrawn: Incorporated into PE-2 and PE-3].

PE-8 ACCESS RECORDS

Control: The organization:
a. Maintains visitor access records to the facility where the information system resides for ***organization-defined time period*****;** and
b. Reviews visitor access records ***at least every 90 days if not otherwise defined in formal organizational policy.***

Control Enhancements:

(1) *VISITOR ACCESS RECORDS* | *AUTOMATED RECORDS MAINTENANCE / REVIEW*
The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

No ICS Supplemental Guidance.

PE-9 POWER EQUIPMENT AND CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Control Enhancements:

(1) *POWER EQUIPMENT AND CABLING* | *REDUNDANT CABLING*
The organization employs redundant power cabling paths that are physically separated by *organization-defined distance, and as required by international, state, and local building codes*.

Supplemental Guidance: Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.

Control Enhancement: (1) No ICS Supplemental Guidance.

Rationale (for adding (1)): Continuity of ICS control and operation requires redundant power cabling.

No ICS Supplemental Guidance.

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in ***organization-defined location by information system or system component, and as required by international, state, and local building codes*** to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

ICS Supplemental Guidance: It may not be possible or advisable to shutoff power to some ICS. Example compensating controls include fail in known state and emergency procedures.

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate ***an orderly shutdown of the information system or transition of the information system to long-term alternate power*** in the event of a primary power source loss.

Control Enhancements:

(1) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*
The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

(2) *EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*
The organization provides a long-term alternate power supply for the information system that is:
(a) Self-contained;
(b) Not reliant on external power generation; and
(c) Capable of maintaining *minimally required operational capability or full operational capability depending on the ICS support mission, and code requirements to remain in an occupied facility for fire, life safety, potable water and sanitary sewage* in the event of an extended loss of the primary power source.

Supplemental Guidance: This control enhancement can be satisfied, for example, by the use of one or more generators with sufficient capacity to meet the needs of the organization. Long-term alternate power supplies for organizational information systems are either manually or automatically activated.

ICS Supplemental Guidance: Emergency power production, transmission and distribution systems are a type of ICS that are required to meet extremely high performance specifications. The systems are governed by international, national, state and local building codes, must be tested on a continual basis, and must be repaired and placed back into operations within a short period of time. Traditionally, emergency power has been provided by generators for short to mid-term power (typically for fire and life safety systems, some IT load, and evacuation transport) and UPS battery packs in distribution closets and within work areas to allow some level of business continuity and for the orderly shutdown of non-essential IT and facility systems. Traditional emergency power systems typically are off-line until a loss of power occurs and are typically on a separate network and control system specific to the facility they support. New methods of energy generation and storage (e.g., solar voltaic, geothermal, flywheel, microgrid, distributed energy) that have a real-time demand and storage connection to local utilities or cross connected to multiple facilities should be carefully analyzed to ensure that the power can meet the load and signal quality without disruption of mission essential functions.

Control Enhancement: (1, 2) No ICS Supplemental Guidance.

Rationale for adding control to baseline: ICS may support critical activities which will be needed for safety and reliability even in the absence of reliable power from the public grid.

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

No ICS Supplemental Guidance.

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Control Enhancements:

(1) *FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*
The organization employs fire detection devices/systems for the information system that activate automatically and notify *organization-defined personnel or roles* and *organization-defined emergency responders* in the event of a fire.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(2) *FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*
The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to *organization-defined personnel or roles* and *organization-defined* emergency responders.

Supplemental Guidance: Organizations can identify specific personnel, roles, and emergency responders in the event that individuals on the notification list must have appropriate access authorizations and/or clearances, for example, to obtain access to facilities where classified operations are taking place or where there are information systems containing classified information.

(3) *FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*
The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

ICS Supplemental Guidance: Fire suppression mechanisms should take the ICS environment into account (e.g., water sprinkler systems could be hazardous in specific environments).

Control Enhancement: (1, 2, 3) No ICS Supplemental Guidance.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:
a. Maintains temperature and humidity levels within the facility where the information system resides at ***organization-defined acceptable levels with temperature and humidity levels within the facility where the ICS resides at typically in the range of 64.4 – 80.6 degrees F; 45% – 60% Relative Humidity; Dew Point 41.9 ° – 59°F***.; and
b. Monitors temperature and humidity levels ***organization-defined frequency***.

ICS Supplemental Guidance: Temperature and humidity controls are typically components of other ICS systems such as the HVAC, process, or lighting systems, or can be a standalone and unique ICS system. ICS can operate in extreme environments and both interior and exterior locations. For a specific ICS, the temperature and humidity design and operational parameters dictate the performance specifications. As ICS and IS become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity.

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Control Enhancements:

(1) *WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*
The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts *organization-defined personnel or roles*.
Supplemental Guidance: Automated mechanisms can include, for example, water detection sensors, alarms, and notification systems.

ICS Supplemental Guidance: Water damage protection and use of shutoff and isolation valves is both a procedural action, and also a specific type of ICS. ICS that are used in the manufacturing, hydropower, transportation/navigation, water and wastewater industries rely on the movement of water and are specifically designed to manage the quantity/flow and pressure of water. As ICS and IS become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems should ensure that water will not disable the system (e.g. a fire that activates the sprinkler system does not spray onto the fire control servers, router, switches and short out the alarms, egress systems, emergency lighting, and suppression systems).

Control Enhancement: (1) No ICS Supplemental Guidance.

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls ***organization-defined types of information system components*** entering and exiting the facility and maintains records of those items.

No ICS Supplemental Guidance.

PE-17 ALTERNATE WORK SITE

Control: The organization:
a. Employs ***organization-defined security controls to include temperature, noise, ventilation and light levels adequate for maintaining a normal level of job performance; stairs with four or more steps must be equipped with handrails; circuit breakers or fuses in the electrical panel are labeled as to the intended service; all electrical equipment must be free of recognized hazards that would cause physical harm (e.g., loose or frayed wires); the building's electrical system***

will permit the grounding of electrical equipment; aisles, doorways, and corners are free of obstructions to permit visibility and movement; file cabinets and storage closets arranged so drawers and doors do not open into walkways; phone lines, electrical cords, and extension wires are secured under a desk or alongside a baseboard; the office space must be neat, clean, and free of excess amounts of combustibles; sufficient light for reading at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

No ICS Supplemental Guidance.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from ***organization-defined physical and environmental hazards to include water, HAZMAT, exhaust hoods and fans, fuel storage areas*** and to minimize the opportunity for unauthorized access.

No ICS Supplemental Guidance.

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
b. Reviews and updates the current:
1. Security planning policy ***at least annually if not otherwise defined in formal organizational policy*** and
2. Security planning procedures ***at least annually if not otherwise defined in formal organizational policy.***

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

PL-2 SYSTEM SECURITY PLAN

Control: The organization:
a. Develops a security plan for the information system that:
1. Is consistent with the organization's enterprise architecture;

2. Explicitly defines the authorization boundary for the system;
3. Describes the operational context of the information system in terms of missions and business processes;
4. Provides the security categorization of the information system including supporting rationale;
5. Describes the operational environment for the information system and relationships with or connections to other information systems;
6. Provides an overview of the security requirements for the system;
7. Identifies any relevant overlays, if applicable;
8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
b. Distributes copies of the security plan and communicates subsequent changes to the plan to ***organization-defined personnel or roles***;
c. Reviews the security plan for the information system ***at least annually or when required due to system modifications***;
d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
e. Protects the security plan from unauthorized disclosure and modification.

Control Enhancements:

(3) *SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*
The organization plans and coordinates security-related activities affecting the information system with *organization-defined individuals or groups* before conducting such activities in order to reduce the impact on other organizational entities.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.

No ICS Supplemental Guidance.

Control Enhancement: (3) No ICS Supplemental Guidance.

Rationale for adding PL-2 (3) to low baseline: When systems are highly inter-connected, coordinated planning is essential. A low impact system could adversely affect a higher impact system.

PL-4 RULES OF BEHAVIOR

Control: The organization:
a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
c. Reviews and updates the rules of behavior ***at least annually or when required due to system modifications***; and
d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Control Enhancements:

(1) *RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.

No ICS Supplemental Guidance.

PL-5 PRIVACY IMPACT ASSESSMENT

[Withdrawn: Incorporated into Appendix J, AR-2].

PL-7 SECURITY CONCEPT OF OPTIONS

Control: The organization:
a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and
b. Reviews and updates the CONOPS ***at least annually or when required due to system modifications.***

No ICS Supplemental Guidance.

Rationale for adding PL-7 to moderate and high baselines: ICS are complex systems. Organizations typically employ a CONOPS to help define a system and share that understanding with personnel involved with that system and other systems with which it interacts. A CONOPS often helps identify information protection requirements.

PL-8 INFORMATION SECURITY ARCHITECTURE

Control: The organization:
a. Develops an information security architecture for the information system that:
1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
3. Describes any information security assumptions about, and dependencies on, external services;
b. Reviews and updates the information security architecture ***at least annually or when required due to system modifications*** to reflect updates in the enterprise architecture; and
c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

No ICS Supplemental Guidance.

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
b. Reviews and updates the current:
1. Personnel security policy ***at least annually if not otherwise defined in formal organizational policy*** and
2. Personnel security procedures ***at least annually if not otherwise defined in formal organizational policy***

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

PS-2 POSITION CATEGORIZATION

Control: The organization:
a. Assigns a risk designation to all organizational positions;
b. Establishes screening criteria for individuals filling those positions; and
c. Reviews and updates position risk designations ***at least annually***.

No ICS Supplemental Guidance.

PS-3 PERSONNEL SCREENING

Control: The organization:
a. Screens individuals prior to authorizing access to the information system; and
b. Rescreens individuals according to ***organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening***.

No ICS Supplemental Guidance.

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:
a. Disables information system access within ***organization-defined time period*;**
b. Terminates/revokes any authenticators/credentials associated with the individual;
c. Conducts exit interviews that include a discussion of ***organization-defined information security topics***;
d. Retrieves all security-related organizational information system-related property;
e. Retains access to organizational information and information systems formerly controlled by terminated individual; and
f. Notifies ***organization-defined personnel or roles*** within ***organization-defined time period***.

Control Enhancements:

(2) *PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*
The organization employs automated mechanisms to notify *organization-defined personnel or roles* upon termination of an individual.
Supplemental Guidance: In organizations with a large number of employees, not all personnel who need to know about termination actions receive the appropriate notifications—or, if such notifications are received, they may not occur in a timely manner. Automated mechanisms can be used to send automatic alerts or notifications to specific organizational personnel or roles (e.g., management personnel, supervisors, personnel security officers, information security officers, systems administrators, or information technology administrators) when individuals are terminated. Such automatic alerts or notifications can be conveyed in a variety of ways, including, for example, telephonically, via electronic mail, via text message, or via websites.

No ICS Supplemental Guidance.

PS-5 PERSONNEL TRANSFER

Control: The organization:
a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b. Initiates actions to ensure all system accesses no longer required (need to know) are removedwithin 24 hours;
c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d. Notifies ***organization-defined personnel or roles*** within ***30 days if not otherwise defined in formal organizational policy***.

No ICS Supplemental Guidance.

PS-6 ACCESS AGREEMENTS

Control: The organization:
a. Develops and documents access agreements for organizational information systems;
b. Reviews and updates the access agreements ***at least annually***; and
c. Ensures that individuals requiring access to organizational information and information systems:
1. Sign appropriate access agreements prior to being granted access; and
2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or ***at least annually.***

No ICS Supplemental Guidance.

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:
a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
b. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
c. Documents personnel security requirements;
d. Requires third-party providers to notify ***organization-defined personnel or roles*** of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within ***organization-defined time period***; and
e. Monitors provider compliance.

No ICS Supplemental Guidance.

PS-8 PERSONNEL SANCTIONS

Control: The organization:
a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
b. Notifies ***organization-defined personnel or roles organization-defined time period*** when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

No ICS Supplemental Guidance.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
b. Reviews and updates the current:
1. Risk assessment policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. Risk assessment procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

RA-2 SECURITY CATEGORIZATION

Control: The organization:
a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

No ICS Supplemental Guidance.

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in ***a risk assessment report or security plan***;
c. Reviews risk assessment results ***at least every 3 years***;
d. Disseminates risk assessment results to ***organization-defined personnel or roles***; and
e. Updates the risk assessment ***at least every 3 years*** or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

No ICS Supplemental Guidance.

RA-5 VULNERABILITY SCANNING

Control: The organization:
a. Scans for vulnerabilities in the information system and hosted applications ***continuously*** and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities ***organization-defined response times*** **in** accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with ***organization-defined personnel or roles to include DHS ICS-CERT*** to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Enhancements:

(1) *VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*
The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.
Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7.

(2) *VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*

The organization updates the information system vulnerabilities scanned *organization-defined frequency, prior to a new scan, or when new vulnerabilities are identified and reported*.

Supplemental Guidance: Related controls: SI-3, SI-5.

(4) *VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*
The organization determines what information about the information system is discoverable by adversaries and subsequently takes *organization-defined corrective actions*.

Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries. Related control: AU-13.

(5) *VULNERABILITY SCANNING | PRIVILEGED ACCESS*
The information system implements privileged access authorization to *organization-identified information system components* for selected *organization-defined vulnerability scanning activities*.

Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning.

ICS Supplemental Guidance: Vulnerability scanning is used with care on ICS systems to ensure that ICS functions are not adversely impacted by the scanning process. The organization makes a risk-based determination whether to employ active scanning. Passive scanning may be used as part of a compensating control. Example compensating controls include providing a replicated, virtualized, or simulated system to conduct scanning. Production ICS may need to be taken off-line before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network.

Control Enhancement: (1, 2, 4, 5) No ICS Supplemental Guidance.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization:

a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
b. Reviews and updates the current:
1. System and services acquisition policy ***at least annually if not otherwise defined in formal organizational policy*** and
2. System and services acquisition procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SA-2 ALLOCATION OF RESOURCES

Control: The organization:
a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

No ICS Supplemental Guidance.

SA-3 LIFE CYCLE SUPPORT

Control: The organization:
a. Determines information security requirements for the information system or information system service in mission/business process planning;
b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

No ICS Supplemental Guidance.

SA-4 ACQUISITIONS

Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system

component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:
a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

Control Enhancements:

(1) *ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5.

(2) *ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*
The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: *security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; organization-defined design/implementation information* at *organization-defined level of detail*.

Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and

hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5.

(9) *ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*
The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

Supplemental Guidance: The identification of functions, ports, protocols, and services early in the system development life cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the information system, information system component, or information system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols, or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols, or services (or when requiring information system service providers to do so). Early identification of functions, ports, protocols, and services avoids costly retrofitting of security controls after the information system, system component, or information system service has been implemented. SA-9 describes requirements for external information system services with organizations identifying which functions, ports, protocols, and services are provided from external sources. Related controls: CM-7, SA-9.

(10) *ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*
The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Supplemental Guidance: Related controls: IA-2; IA-8.

ICS Supplemental Guidance: Since ICS security has historically focused on physical protection and isolation, vendors and developers may be unfamiliar with cybersecurity. Organizations should anticipate a need to engage with ICS suppliers to raise awareness of cybersecurity needs. The SCADA/Control Systems Procurement Project provides example cyber security procurement language for ICS. References: Web: http://ics-cert.us-cert.gov/sites/default/files/FINAL-Procurement_Language_Rev4_100809_0.pdf

Control Enhancements: (1, 2, 9) ICS Supplemental Guidance: Developers may not have access to required information.

Control Enhancement: (10) ICS Supplemental Guidance: Example compensating controls include employing external products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability in conjunction with ICS products.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:
a. Obtains administrator documentation for the information system, system component, or information system service that describes:
1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security functions/mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b. Obtains user documentation for the information system, system component, or information system service that describes:
1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
3. User responsibilities in maintaining the security of the system, component, or service;
c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and ***notifies the Chief Information Officer*** in response;
d. Protects documentation as required, in accordance with the risk management strategy; and
e. Distributes documentation to ***organization-defined personnel or roles***.

No ICS Supplemental Guidance.

SA-6 SOFTWARE USAGE RESTRICTIONS

[Withdrawn: Incorporated into CM-10 and SI-7].

SA-7 USER INSTALLED SOFTWARE

[Withdrawn: Incorporated into CM-11 and SI-7].

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

No ICS Supplemental Guidance.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ ***organization-defined***

security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs ***organization-defined processes, methods, and techniques*** **to** monitor security control compliance by external service providers on an ongoing basis.

Control Enhancements:

(2) *EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*
The organization requires providers of *organization-defined external information system services* to identify the functions, ports, protocols, and other services required for the use of such services.

Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7.

No ICS Supplemental Guidance.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires the developer of the information system, system component, or information system service to:
a. Perform configuration management during system, component, or service ***design; development; implementation; or operation***;
b. Document, manage, and control the integrity of changes to ***organization-defined configuration items under configuration management***;
c. Implement only organization-approved changes to the system, component, or service;
d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e. Track security flaws and flaw resolution within the system, component, or service and report findings to ***organization-defined personnel***.

No ICS Supplemental Guidance.

SA-11 DEVELOPER SECURITY TESTING

Control: The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ ***organization-defined security controls*** in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Employs ***organization-defined processes, methods, and techniques*** to monitor security control compliance by external service providers on an ongoing basis.

No ICS Supplemental Guidance.

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats to the information system, system component, or information system service by employing ***measures in accordance with CNSS Directive 505, Supply Chain Risk Management*** as part of a comprehensive, defense-in-breadth information security strategy.

No ICS Supplemental Guidance.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Control: The organization:
a. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
1. Explicitly addresses security requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
b. Reviews the development process, standards, tools, and tool options/configurations ***organization-defined frequency*** to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy ***organization-defined security requirements***.

No ICS Supplemental Guidance.

SA-16 DEVELOPER –PROVIDED TRAINING

Control: The organization requires the developer of the information system, system component, or information system service to provide ***organization-defined training*** on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

No ICS Supplemental Guidance.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:
a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;
b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

No ICS Supplemental Guidance.

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
b. Reviews and updates the current:
1. System and communications protection policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. System and communications protection procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SC-2 APPLICATION PARTIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

ICS Supplemental Guidance: Systems used to manage the ICS should be separate from the operational ICS components. Example compensating controls include providing increased auditing measures.

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures, limiting network connectivity, architectural allocation.

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

ICS Supplemental Guidance: Example compensating controls include architecting the use of the ICS to prevent sharing system resources.

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: ***Consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, physical destruction or alteration of network components*** by employing ***organization-defined security safeguards***.

ICS Supplemental Guidance: Example compensating controls include ensuring a loss of communication results in the ICS operating in nominal or safe mode. Risk-based analysis informs the establishment of policy and procedure.

SC-7 BOUNDARY PROTECTION

Control: The information system:
a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
b. Implements subnetworks for publicly accessible system components that are ***physically or logically*** separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

(3) *BOUNDARY PROTECTION | ACCESS POINTS*
The organization limits the number of external network connections to the information system.

Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections.

(4) *BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*
The organization:
(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;
(c) Protects the confidentiality and integrity of the information being transmitted across each interface;
(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
(e) Reviews exceptions to the traffic flow policy *at least every 6 months* and removes exceptions that are no longer supported by an explicit mission/business need.

Supplemental Guidance: Related control: SC-8.

(5) *BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*
The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

(7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES
The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

(8) *BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*
The information system routes *all internal communications traffic, except traffic specifically exempted by the Authorizing Official or organizational policy* to

networks outside the control of the organization **through authenticated proxy servers at managed interfaces.**

Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity. Web content filtering devices are one of the most common proxy servers providing access to the Internet. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Web proxies can be configured with organization-defined lists of authorized and unauthorized websites. Related controls: AC-3, AU-2.

(18) *BOUNDARY PROTECTION | FAIL SECURE*
The information system fails securely in the event of an operational failure of a boundary protection device.

Supplemental Guidance: Fail secure is a condition achieved by employing information system mechanisms to ensure that in the event of operational failures of boundary protection devices at managed interfaces (e.g., routers, firewalls, guards, and application gateways residing on protected subnetworks commonly referred to as demilitarized zones), information systems do not enter into unsecure states where intended security properties no longer hold. Failures of boundary protection devices cannot lead to, or cause information external to the devices to enter the devices, nor can failures permit unauthorized information releases. Related controls: CP-2, SC-24.

(21) *BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*
The organization employs boundary protection mechanisms to separate ***organization-defined information system components*** **supporting** ***organization-defined missions and/or business functions*****.**

Supplemental Guidance: Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or subnetworks, cross-domain devices separating subnetworks,

virtualization techniques, and encrypting information flows among system components using distinct encryption keys. Related controls: CA-9, SC-3.

No ICS Supplemental Guidance.

Control Enhancement: (3, 4, 5, 7, 8, 21) No ICS Supplemental Guidance.

Control Enhancement: (18) ICS Supplemental Guidance: The organization selects an appropriate failure mode (e.g., permit or block all communications).

Rationale for adding SC-7 (18) to Moderate Baseline: As part of the architecture and design of the ICS, the organization selects an appropriate failure mode in accordance with the function performed by the ICS and the operational environment. The ability to choose the failure mode for the physical part of the ICS differentiates the ICS from other IT systems. This choice may be a significant influence in mitigating the impact of a failure.

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the ***confidentiality and/or integrity*** of transmitted information.

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*
The information system implements cryptographic mechanisms to *prevent unauthorized disclosure of information or detect changes to information* during transmission unless otherwise protected by *organization-defined alternative physical safeguards*.

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: The organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function). Each mechanism has a different delay impact.

SC-9 TRANSMISSION CONFIDENTIALITY

[Withdrawn: Incorporated into SC-8].

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after ***not more than 1 hour*** of inactivity.

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with ***organization-defined requirements for key generation, distribution, storage, access, and destruction***.

Control Enhancements:

(1) *CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*
The organization maintains availability of information in the event of the loss of cryptographic keys by users.

Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase).

ICS Supplemental Guidance: The use of cryptographic key management in ICS is intended to support internal nonpublic use.

Control Enhancement: (1) No ICS Supplemental Guidance.

SC-13 USE OF CRYPTOGRAPHY

Control: The information system implements ***organization-defined cryptographic uses and type of cryptography required for each use*** in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

No ICS Supplemental Guidance.

SC-14 PUBLIC ACCESS PROTECTIONS

[Withdrawn: Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:
a. Prohibits remote activation of collaborative computing devices with the following exceptions: ***remote activation of centrally managed dedicated VTC Suites located in approved VTC locations***; and
b. Provides an explicit indication of use to users physically present at the devices.

No ICS Supplemental Guidance.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an ***organization-defined certificate policy*** or obtains public key certificates from an approved service provider.

No ICS Supplemental Guidance.

SC-18 MOBILE CODE

Control: The organization:
a. Defines acceptable and unacceptable mobile code and mobile code technologies;
b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c. Authorizes, monitors, and controls the use of mobile code within the information system.

No ICS Supplemental Guidance.

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:
a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
b. Authorizes, monitors, and controls the use of VoIP within the information system.

ICS Supplemental Guidance: The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system:
a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION (RECURSIVE OR CAHING RESOLVER)

Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-23 SESSSION AUTHENTICITY

Control: The information system protects the authenticity of communications sessions.

ICS Supplemental Guidance: Example compensating controls include auditing measures.

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a ***known secure state*** for ***all types of failures*** preserving, ***information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes*** in failure.

ICS Supplemental Guidance: The organization selects an appropriate failure state. Preserving ICS state information includes consistency among ICS state variables and

the physical state which the ICS represents (e.g., whether valves are open or closed, communication permitted or blocked, continue operations).

Rationale for adding SC-24 to moderate baseline: As part of the architecture and design of the ICS, the organization selects an appropriate failure state of an ICS in accordance with the function performed by the ICS and the operational environment. The ability to choose the failure mode for the physical part of the ICS differentiates the ICS from other IT systems. This choice may be a significant influence in mitigating the impact of a failure, since it may be disruptive to ongoing physical processes (e.g., valves failing in closed position may adversely affect system cooling).

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the ***confidentiality and/or integrity*** of ***organization-defined information at rest***.

ICS Supplemental Guidance. The use of cryptographic mechanisms is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-33 TRANSMISSION PREPARATION INTEGRITY

[Withdrawn: Incorporated into SC-8].

SC-39 PROCESS ISOLATION

Control: The information system maintains a separate execution domain for each executing process.

ICS Supplemental Guidance: Example compensating controls include partition processes to separate platforms.

SC-41 PORT AND I/O DEVICE ACCESS

Control: The organization physically disables or removes ***organization-defined connection ports or input/output devices*** on ***organization-defined information systems or information system components***.

No ICS Supplemental Guidance.

Rationale for adding SC-24 to all baselines: The function of ICS can be readily determined in advance, making it easier to identify ports and I/O devices that are unnecessary. Disabling or removing ports reinforces air-gap policy.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization:
a. Develops, documents, and disseminates to ***organization-defined personnel or roles***:
1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
b. Reviews and updates the current:
1. System and information integrity policy ***at least annually if not otherwise defined in formal organizational policy***; and
2. System and information integrity procedures ***at least annually if not otherwise defined in formal organizational policy***.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SI-2 FLAW REMEDIATION

Control: The organization:
a. Identifies, reports, and corrects information system flaws;
b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Installs security-relevant software and firmware updates within ***organization-defined time period*** of the release of the updates; and
d. Incorporates flaw remediation into the organizational configuration management process.

Control Enhancements:

(1) *FLAW REMEDIATION | CENTRAL MANAGEMENT*
The organization centrally manages the flaw remediation process.

Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls.

(2) *FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*
The organization employs automated mechanisms *organization-defined frequency* to determine the state of information system components with regard to flaw remediation.

Supplemental Guidance: Related controls: CM-6, SI-4.

ICS Supplemental Guidance: Flaw Remediation is complicated since many ICS employ operating systems and other software that is not current, is no longer being maintained by the vendors, and is not resistant to current threats. ICS operators are often dependent on product vendors to validate the operability of a patch and also sometimes to perform the installation. Often flaws cannot be remediated based on circumstances outside of the ICS operator's control (e.g., lack of a vendor patch). Sometime the organization has no choice but to accept additional risk. In these situations, compensating controls should be implemented (e.g., limit the exposure of the vulnerable system). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident; devise a plan to ensure the ICS can identify the exploitation of the flaw). Testing flaw remediation in an ICS may require more resources than the organization can commit.

Control Enhancement: (1) No ICS Supplemental Guidance.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures which incorporate methods to apply, track, and verify mitigation efforts as compensating controls in accordance with the general tailoring guidance.

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:
a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c. Configures malicious code protection mechanisms to:
1. Perform periodic scans of the information system ***at least weekly*** and real-time scans of files from external sources at ***endpoint or network entry/exit points*** as the files are downloaded, opened, or executed in accordance with organizational security policy; and
2. ***Quarantine malicious code and send an alert to the system administrator*** in response to malicious code detection; and
d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system .

Control Enhancements:

(1) *MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*
The organization centrally manages malicious code protection mechanisms.

Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management

includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8.

(2) *MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*
The information system automatically updates malicious code protection mechanisms.

Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8.

ICS Supplemental Guidance: The use and deployment of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS. Malicious code protection tools should be configured to minimize their potential impact on the ICS (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

Control Enhancement: (1) ICS Supplemental Guidance: The organization implements central management of malicious code protection with consideration of the impact on operation of the ICS. Example compensating controls include increased auditing.

Control Enhancement: (2) ICS Supplemental Guidance: The organization implements automatic updates of malicious code protection with consideration of the impact on operation of the ICS. In situations where the ICS cannot support the use of automatic update of malicious code protection, the organization employs nonautomated procedures as compensating controls in accordance with the general tailoring guidance.

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:
a. Monitors the information system to detect:
1. Attacks and indicators of potential attacks in accordance with ***organization-defined monitoring objectives***; and
2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of the information system through ***organization-defined techniques and methods***;
c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other

organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
g. Provides ***organization-defined information system monitoring information*** to ***organization-defined personnel or roles*****,** ***as needed, or organization-defined frequency***.

Control Enhancements:

(2) *INFORMATION SYSTEM MONITORING* | *AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*
The organization employs automated tools to support near real-time analysis of events.

Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems.

(4) *INFORMATION SYSTEM MONITORING* | *INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*
The information system monitors inbound and outbound communications traffic *organization-defined frequency* for unusual or unauthorized activities or conditions.

Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or propagating among system components, the unauthorized exporting of information, or potentially compromised information systems or information system components.

(5) *INFORMATION SYSTEM MONITORING* | *SYSTEM-GENERATED ALERTS*
The information system alerts *organization-defined personnel or roles* when the following indications of compromise or potential compromise occur: *organization-defined compromise indicators*.

Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business

owners, system owners, or information system security officers. Related controls: AU-5, PE-6.

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS. Example compensating controls include deploying sufficient network monitoring.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

Control Enhancement: (4) ICS Supplemental Guidance: In situations where the ICS cannot monitor inbound and outbound communications traffic, the organization employs compensating controls include providing a monitoring capability on a separate information system.

Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include manual methods of generating alerts.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:
a. Receives information system security alerts, advisories, and directives from ***organization-defined external organizations***, ***but minimum with DHS ICS-CERT,*** on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to: ***organization-defined personnel or roles***, ***organization-defined elements within the organization*****,** ***organization-defined external organizations***; and
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Control Enhancements:

(1) *SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*
The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Supplemental Guidance: The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may

be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.

ICS Supplemental Guidance: The DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) generates security alerts and advisories relative to ICS http://ics-cert.us-cert.gov/ .

Control Enhancement: (1) No ICS Supplemental Guidance.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system:
a. Verifies the correct operation of ***organization-defined security functions***;
b. Performs this verification ***organization-defined system transitional states, upon command by user with appropriate privilege, organization-defined frequency***;
c. Notifies ***organization-defined personnel or roles*** of failed security verification tests; and
d. ***Shuts the information system down, restarts the information system, or organization-defined alternative action(s)*** when anomalies are discovered.

ICS Supplemental Guidance: The shutting down and restarting of the ICS may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to ICS operational requirements.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The organization employs integrity verification tools to detect unauthorized changes to ***organization-defined software, firmware, and information***.

Control Enhancements:

(1) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*
The information system performs an integrity check of *organization-defined software, firmware, and information* at *startup*, at *organization-defined transitional states or security-relevant events*, *organization-defined frequency*.

Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort.

(2) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*

The organization employs automated tools that provide notification to *organization-defined personnel or roles* upon discovering discrepancies during integrity verification.

Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers.

(5) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*
The information system automatically *shuts the information system down, restarts the information system or implements organization-defined security safeguards* when integrity violations are discovered.

Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur.

(7) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*
The organization incorporates the detection of unauthorized *organization-defined security-relevant changes to the information system* into the organizational incident response capability.

Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4.

(14) *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*
The organization:
(a) Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official.

Supplemental Guidance: This control enhancement applies to all sources of binary or machine-executable code including, for example, commercial software/firmware and open source software. Organizations assess software products without accompanying source code from sources with limited or no warranty for potential security impacts. The assessments address the fact that these types of software products may be very difficult to review, repair, or extend, given that organizations, in most cases, do not have access to the original source code, and there may be no owners who could make such repairs on behalf of organizations. Related control: SA-5.

ICS Supplemental Guidance: The organization determines whether the use of integrity verification applications would adversely impact the operation of the ICS and employs compensating controls (e.g., manual integrity verifications that do not affect performance.

Control Enhancements: (1) ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

Control Enhancement: (5) ICS Supplemental Guidance: The shutting down and restarting of the ICS may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to ICS operational requirements.

Control Enhancement: (7) ICS Supplemental Guidance: In situations where the ICS cannot detect unauthorized security-relevant changes, the organization employs compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

Control Enhancement: (14) No ICS Supplemental Guidance.

SI-8 SPAM PROTECTION

Control: The organization:
a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Control Enhancements:

(1) *SPAM PROTECTION | CENTRAL MANAGEMENT*

The organization centrally manages spam protection mechanisms.
Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7.

(2) *SPAM PROTECTION | AUTOMATIC UPDATES*
The information system automatically updates spam protection mechanisms.

ICS Supplemental Guidance: ICS spam protection may be implemented by removing spam transport mechanisms, functions and services (e.g., electronic mail, Internet access) from the ICS. If any spam transport mechanisms, functions and services are present in the ICS, spam protection in ICS takes into account operational characteristics of ICS that differ from general purpose information systems, (e.g., unusual traffic flow that may be misinterpreted and detected as spam. Example compensating controls include whitelist mail transfer agents (MTA), digitally signed messages, acceptable sources, and acceptable message types.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include employing local mechanisms or procedures.

SI-9 INFORMATION INPUT RESTRICTIONS

[Withdrawn: Incorporated into AC-2, AC-3, AC-5, AC-6].

SI-10 INFORMATION INOUT VALIDATION

Control: The information system checks the validity of ***organization-defined information inputs***.

No ICS Supplemental Guidance.

SI-11 ERROR HANDLING

Control: The information system:
a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
b. Reveals error messages only to ***organization-defined personnel or roles***.

No ICS Supplemental Guidance.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws,

Executive Orders, directives, policies, regulations, standards, and operational requirements.

No ICS Supplemental Guidance.

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:
a. Determines mean time to failure (MTTF) for ***organization-defined information system components*** in specific environments of operation; and
b. Provides substitute information system components and a means to exchange active and standby components at ***organization-defined MTTF substitution criteria***.

ICS Supplemental Guidance: Failures in ICS can be stochastic or deterministic. Stochastic failures can be analyzed using probability theory, while analysis of deterministic failures is based on non-random properties of the system. Known ICS failure modes and causes are considered. The calculation and use of statistical descriptors, such as Mean Time To Failure (MTTF), should incorporate additional analysis to determine how those failures manifest within the cyber and physical domains. Knowledge of these possible manifestations may be necessary to detect whether a failure has occurred within the ICS, as failures of the information systems may not easily identifiable. Emergent properties, which may arise both within the information systems and physical processes, can potentially cause system failures should be incorporated into the analysis. For example, cumulative effects of resource exhaustion (e.g., memory leakage) or errors (e.g., rounding and truncation) can occur when ICS processes execute for unexpectedly long periods. Deterministic failures (e.g., integer counter overflow), once identified, are preventable.

Often substitute components may not be available or may not be sufficient to protect against faults occurring before predicted failure. Non-automated mechanisms or physical safeguards should be in place in order to protect against these failures.
In addition to information concerning newly discovered vulnerabilities (i.e., latent flaws) potentially affecting the system/applications that are discovered by forensic studies, new vulnerabilities may be identified by organizations with responsibility for disseminating vulnerability information (e.g., ICS-CERT) based upon an analysis of a similar pattern of incidents reported to them or vulnerabilities reported by other researchers.

SI-16 MEMORY PROTECTION

Control: The information system implements ***organization-defined security safeguards*** to protect its memory from unauthorized code execution.

No ICS Supplemental Guidance.

SI-17 FAIL-SAFE PROCEDURES

Control: The information system implements ***organization-defined fail-safe procedures*** when ***organization-defined failure conditions occur***.

ICS Supplemental Guidance: The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different response depending on the impact level. Mechanical and analog system can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. Related controls: CP-6.

Rationale for adding SI-17 to all baselines: This control provides a structure for the organization to identify their policy and procedures for dealing with failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control: The organization:
a. Develops and disseminates an organization-wide information security program plan that:
1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
b. Reviews the organization-wide information security program ***at least annually if not otherwise defined in formal organizational policy***;
c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
d. Protects the information security program plan from unauthorized disclosure and modification.

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS, the relationship to non-ICS systems, and the relationship to other programs concerned with operational characteristics of ICS (e.g., safety, efficiency, reliability, resilience).

PM-2 SENIOR INFORMATION SECURITY OFFICER

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

No ICS Supplemental Guidance.

PM-3 INFORMATION SECURITY RESOURCES

Control: The organization:
a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
c. Ensures that information security resources are available for expenditure as planned.

ICS Supplemental Guidance: Capital planning and investment decisions address all of the relevant technologies and all phases of the life cycle and needs to be informed by ICS experts as well as other subject matter experts (e.g., information security). Marshaling interdisciplinary working teams to advise capital planning and investment decisions can help tradeoff and balance among conflicting equities, objectives, and responsibilities such as capability, adaptability, resiliency, safety, security, usability, and efficiency.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The organization:
a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
1. Are developed and maintained;
2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with OMB FISMA reporting requirements.
b. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

ICS Supplemental Guidance: The plan of action and milestones includes both computational and physical ICS components. Records of observed shortcomings and appropriate remedial action may be maintained in a single document or in multiple coordinated documents (e.g., future engineering plans).

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

No ICS Supplemental Guidance.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

No ICS Supplemental Guidance.

PM-7 ENTERPRISE ARCHITECTURE

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

ICS Supplemental Guidance: [Note to reviewers; This SG will address ICS architecture relationship to information security architecture, drawn from body of SP 800-82 when written.]

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

ICS Supplemental Guidance: [Note to reviewers; This SG will address ICS architecture relationship to information security architecture, drawn from body of SP 800-82 when written.]

PM-9 RISK MANAGEMENT STRATEGY

Control: The organization:
a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
b. Implements the risk management strategy consistently across the organization; and
c. Reviews and updates the risk management strategy ***at least annually if not otherwise defined in formal organizational policy*** or as required, to address organizational changes.

ICS Supplemental Guidance: Risk management of ICS is considered along with other organizational risks affecting mission/business success from an organization-wide perspective. Organization-wide risk management strategy includes sector-specific guidance as appropriate.

PM-10 SECURITY AUTHORIZATION PROCESS

Control: The organization:
a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
c. Fully integrates the security authorization processes into an organization-wide risk management program.

ICS Supplemental Guidance: The authorization to operate processes for ICS involve multiple disciplines that have existing approval and risk management process (e.g., physical security, safety). Organization-wide risk management requires harmonization among these disciplines.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control: The organization:
a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

ICS Supplemental Guidance: Mission/business processes refinement requires protection of physical assets from damage originating in the cyber domain. These needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy.

PM-12 INSIDER THREAT PROGRAM

Control: The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.

No ICS Supplemental Guidance.

PM-13 INFORMATION SECURITY WORKFORCE

Control: The organization establishes an information security workforce development and improvement program.

ICS Supplemental Guidance: All aspects of information security workforce development and improvement programs includes knowledge and skill levels in both computational and physical ICS components.

PM-14 TESTING, TRAINING, AND MONITORING

Control: The organization:
a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
1. Are developed and maintained; and
2. Continue to be executed in a timely manner;
b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

No ICS Supplemental Guidance.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:
a. To facilitate ongoing security education and training for organizational personnel;
b. To maintain currency with recommended security practices, techniques, and technologies; and
c. To share current security-related information including threats, vulnerabilities, and incidents.

No ICS Supplemental Guidance.

PM-16 THREAT AWARENESS PROGRAM

Control: The organization implements a threat awareness program that includes a cross-organization information-sharing capability.

No ICS Supplemental Guidance.