Appendix G—ICS Overlay

Note to Reviewers

Revision 1 to NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, was published in May 2013. Updates in this revision include the integration of the Appendix I ICS material transferred from NIST SP 800-53, Revision 3. This material is now located in Appendix G of SP 800-82, Revision 1.

NIST is developing Revision 2 to SP 800-82 that will include:

- Updates to ICS threats and vulnerabilities;
- Updates to ICS risk management, recommended practices and architectures;
- Updates to current activities in ICS security;
- Updates to security capabilities and technologies for ICS;
- Additional alignment with other ICS security standards and guidelines;
- New tailoring guidance for NIST SP 800-53, Revision 4 security controls including introduction of overlays; and
- ICS overlay for NIST SP 800-53, Revision 4 security controls that will provide tailored security control baselines for Low, Moderate, and High impact ICS.

This document is a preliminary draft of the ICS overlay. When SP 800-82, Revision 2 is published, this ICS overlay will be included as an Appendix. The genesis of this overlay is contained in NIST Special Publication 800-53, Revision 4, published April 2013, which represents the culmination of a two-year initiative to update the guidance for the selection and specification of security controls for federal information systems and organizations. The ICS overlay is a partial tailoring of the controls and control baselines in SP 800-53, Revision 4, and adds supplementary guidance specific to ICS. The concept of overlays is introduced in Appendix I of SP 800-53, Revision 4. The ICS overlay is intended to be applicable to all ICS systems in all industrial sectors. Further tailoring can be performed to add specificity to a particular sector (e.g., pipeline, energy). Ultimately, an overlay may be produced for a specific system (e.g., the XYZ company). This ICS overlay constitutes supplemental guidance and tailoring for SP 800-53, Revision 4. Please be sure you are looking at the correct version of SP 800-53. Duplicating Appendix F of SP 800-53 would increase the size of this document by over 65 pages. Therefore, the drafting committee has decided to not duplicate Appendix F. The reader should have SP 800-53, Revision 4 available. The authoring team also considered that this ICS overlay may serve as a model for other overlays. Feedback on this document structure would be appreciated, especially in the following areas: the level of abstraction and whether the examples provided in the supplemental guidance are sufficient/beneficial for implementation.

The body of SP 800-82, Revision 2 is in development at this time. Sections of the ICS overlay that are dependent on material from the body of SP 800-82, Revision 2 are appropriately identified; these sections will be completed in a future draft of the ICS overlay. This draft is being made available at this time for controlled distribution among an identified set of subject

matter experts to stimulate information sharing and feedback. We would like to express our sincere appreciation to the many organizations and individuals in the public and private sectors who are contributing their time and expertise to submit comments on this draft of the ICS overlay. At this early stage in the development of SP 800-82, Revision 2, of which this overlay is a part, comments on structure, organization, and level of detail are most useful.

Since the ICS overlay exists in the context of SP 800-53, Revision 4, it is important to review that context. SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, represents the most comprehensive update to the security controls catalog since its inception in 2005. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the concept of overlays was introduced in this revision. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

Finally, there have been several new features added to this revision to facilitate ease of use by organizations. These include:

- Assumptions relating to security control baseline development;
- Expanded, updated, and streamlined tailoring guidance;
- Additional assignment and selection statement options for security and privacy controls;
- Descriptive names for security and privacy control enhancements;
- Consolidated tables for security controls and control enhancements by family with baseline allocations;
- Tables for security controls that support development, evaluation, and operational assurance; and
- Mapping tables for international security standard ISO/IEC 15408 (Common Criteria).

Again, NIST would like to express its sincere appreciation to the many organizations and individuals in the public and private sectors who are contributing their time and expertise to submit comments on this draft of the ICS overlay. At this early stage in the development of SP 800-82, Revision 2, of which this overlay is a part, comments on structure, organization, and level of detail are most useful.

Keith Stouffer, Project Leader
Intelligent Systems Division
Engineering Laboratory
National Institute of Standards and Technology

Identification

This overlay may be referenced as the NIST Special Publication 800-82 revision 2 Industrial Control System Overlay, abbreviated NIST SP 800-82 rev 2 ICS Overlay. It is based on SP 800-53 revision 4, published April 30, 2013.

The National Institute of Standards and Technology (NIST) developed this Overlay, which is contained in SP 800-82 rev 2, in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, Presidential Policy Directive (PPD)-21 and Executive Order 13636. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. Comments may be directed to icsoverlaycomments@nist.gov.

This Overlay remains in effect until further notice.

Overlay Characteristics

[Note to reviewers: This section has not yet been written. It will incorporate the following guidance from SP 800-53 Appendix I.]

Organizations describe the characteristics that define the intended use of the overlay in order to help potential users select the most appropriate overlay for their missions/business functions. This may include, for example, a description of: (i) the environment in which the information system will be used (e.g., inside a guarded building within the continental United States, in an unmanned space vehicle, while traveling for business to a foreign country that is known for attempting to gain access to sensitive or classified information, or in a mobile vehicle that is in close proximity to hostile entities); (ii) the type of information that will be processed, stored, or transmitted (e.g., personal identity and authentication information, financial management information, facilities, fleet, and equipment management information, defense and national security information, system development information); (iii) the functionality within the information system or the type of system (e.g., standalone system, industrial/process control system, or cross-domain system); and (iv) other characteristics related to the overlay that help protect organizational missions/business functions, information systems, information, or individuals from a specific set of threats that may not be addressed by the assumptions described in Chapter Three (of SP 800-53 rev 4).

Applicability

The purpose of this overlay is to provide guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLCs), and other systems performing industrial control functions. This overlay has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis.

Overlay Summary

Table G-1 provides a summary of the security controls and control enhancements from SP 800-53 Appendix F that have been allocated to the initial security control baselines (i.e., Low, Moderate, and High) along with indications of ICS Supplemental Guidance and ICS tailoring. Controls and control

enhancements for which there is ICS Supplemental Guidance are bolded. If the control baselines are supplemented by the addition of a control to the baseline, the control or control enhancement is underlined. If a control or control enhancement is removed from the baseline, the control or control enhancement is struck out.

Example:

AU-4	Audit Storage Capacity	AU-4 (1)	AU-4 (1)	AU-4 (1)

In this example, ICS Supplemental Guidance was added to Control Enhancement 1 of AU-4 (bolded). In addition, Control Enhancement 1 of AU-4 was added to the Low, Mod, and High baselines (underlined).

TABLE G-1: SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (12) (13)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	Not Selected	AC-12	AC-12
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Collaboration and Information Sharing	Added	AC-21	AC-21
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	AT-2	AT-2 (2)	AT-2 (2)

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AT-3	Role-Based Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Audit Events	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 (1) (3)
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	CA-3	CA-3 (5)	CA-3 (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	CA-9	CA-9	CA-9
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	CM-7 (1)	CM-7 (1) (2) ~~(4)~~ (5)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	CM-10	CM-10	CM-10
CM-11	User-Installed Software	CM-11	CM-11	CM-11
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
CP-2	Contingency Plan	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-12	Safe Mode	CP-12	CP-12	CP-12
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	IA-3	IA-3 (1) (4)	IA-3 (1) (4)
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3	MP-3

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	MP-7	MP-7 (1)	MP-7 (1)
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1) (4)	PE-6 (1) (4)
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	PE-9 (1)	PE-9 (1)
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10
PE-11	Emergency Power	PE-11 (1)	PE-11 (1)	PE-11 (1) (2)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected	PE-18
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4 (1)	PL-4 (1)
PL-7	Security Concept of Operations		PL-7	PL-7
PL-8	Information Security Architecture	Not Selected	PL-8	PL-8
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	SA-5	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-15	Development Process, Standards, and Tools	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	SA-17
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) (18)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8 (1)	SC-8 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	Not Selected	SC-24	SC-24
SC-28	Protection of Information at Rest	Not Selected	SC-28	SC-28
SC-39	Process Isolation	SC-39	SC-39	SC-39
SC-41	Port and I/O Device Access	SC-41	SC-41	SC-41
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	Information Input Validation	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	SI-13
SI-14	Non-Persistence	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	SI-17	SI-17	SI-17

The PM-family is deployed organization-wide, supporting the information security program. It is not associated with security control baselines and is independent of any system impact level.

PM-1	Information Security Program Plan	PM-1
PM-2	Senior Information Security Officer	PM-2
PM-3	Information Security Resources	PM-3
PM-4	Plan of Action and Milestones Process	PM-4
PM-5	Information System Inventory	PM-5
PM-6	Information Security Measures of Performance	PM-6
PM-7	Enterprise Architecture	PM-7
PM-8	Critical Infrastructure Plan	PM-8
PM-9	Risk Management Strategy	PM-9
PM-10	Security Authorization Process	PM-10
PM-11	Mission/Business Process Definition	PM-11
PM-12	Insider Threat Program	PM-12
PM-13	Information Security Workforce	PM-13
PM-14	Testing, Training, and Monitoring	PM-14
PM-15	Contacts with Security Groups and Associations	PM-15
PM-16	Threat Awareness Program	PM-16

Tailoring Considerations

Due to the unique characteristics of ICS, these systems may require a greater use of compensating security controls than is the case for general purpose information systems. Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. See "Selecting Compensating Security Controls" in section 3.2 of SP 800-53 revision 4.

In situations where the ICS cannot support, or the organization determines it is not advisable to implement, particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.

In accordance with the Technology-related Considerations of the Scoping Guidance in SP 800-53, Revision 4, section 3.2, if automated mechanisms are not readily available, cost-effective, or technically feasible in the ICS, compensating security controls, implemented through nonautomated mechanisms or procedures are employed.

Compensating controls are alternative security controls employed by organizations in lieu of specific controls in the baselines—controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems.[1] This may occur, for example, when organizations are unable to effectively implement specific security controls in the baselines or when, due to the specific nature of the ICS or environments of operation, the controls in the baselines are not a cost-effective means of obtaining the needed risk mitigation. Compensating controls may include control enhancements that supplement the baseline. Using compensating controls may involve a trade-off between additional risk and reduced functionality. Every use of compensating controls should involve a risk-based determination of: (i) how much residual risk to accept, and (ii) how much functionality should be reduced. Compensating controls may be employed by organizations under the following conditions:

- Organizations select compensating controls from SP 800-53, Appendix F. If appropriate compensating controls are not available, organizations adopt suitable compensating controls from other sources;[2]
- Organizations provide supporting rationale for how compensating controls provide equivalent security capabilities for organizational information systems and why the baseline security controls could not be employed; and
- Organizations assess and accept the risk associated with implementing compensating controls in ICS.

Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

[1] More than one compensating control may be required to provide the equivalent protection for a particular security control in Appendix F. For example, organizations with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls.
[2] Organizations should make every attempt to select compensating controls from the security control catalog in Appendix F. Organization-defined compensating controls are employed *only* when organizations determine that the security control catalog does not contain suitable compensating controls.

Controls that contain assignments (e.g., *Assignment: organization-defined conditions or trigger events*) may be tailored out of the baseline. This is equivalent to assigning a value of "none." The assignment may take on different values for different impact baselines.

Definitions

Terms used in this overlay are defined in Appendix B or in NIST Interagency Report (NISTIR 7298) Revision 2, Glossary of Key Information Security Terms.

Additional Information or Instructions

[Note to reviewers: This section has not yet been written. It will incorporate the following guidance from SP 800-53 Appendix I.]

Organizations provide any additional information or instructions relevant to the overlay not covered in the previous sections.

Detailed Overlay Control Specifications

This Overlay is based on the NIST SP 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and assurance helps to ensure that information technology component products and the information systems built from those products using sound system and security engineering principles are sufficiently trustworthy.

In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. This process is known as security categorization. FIPS 199 enables federal agencies to establish security categories for both information and information systems. Other documents, such as those produced by ISA and CNSS, also provide guidance for defining low, moderate, and high levels of security based on impact. The security categories are based on the potential impact on an organization or on people (employees and/or the public) should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals' safety, health and life. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

This Overlay provides ICS Supplemental Guidance for the security controls and control enhancements prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. This Overlay contains a tailoring of the security control baselines; its specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. This Overlay is high-level, applicable to all ICS; it may be used as the basis for more specific overlays. Use cases for specific systems in specific environments may be separately published (e.g., as a NISTIR).

Figure G-1 uses the AU-4 control as an example of the format and content of the detailed overlay control specifications.

❶ Control number and title.
❷ Column for control and control enhancement number.
❸ Column for control and control enhancement name.
❹ Columns for baselines. If the baselines have been supplemented, then SUPPLEMENTED appears.
❺ A row for each control or control enhancement.
❻ Columns for LOW, MODERATE, and HIGH baselines.
❼ If the control is selected in SP 800-53 rev 4, then Selected appears. If the control is added to a baseline in the ICS overlay, then Added appears. If the control is not selected, then the cell is blank. If the control is removed from the baseline, then Removed appears.
❽ The ICS Supplemental Guidance. If there is none, that is stated.
❾ The Control Enhancement ICS Supplemental Guidance. If there is none, that is stated.
❿ The rationale for changing the presence of a control or control enhancement in the baseline.

❶ AU-4 AUDIT STORAGE CAPACITY

❷ CNTL NO.	❸ CONTROL NAME *Control Enhancement Name*	❹ SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	Audit Storage Capacity	Selected	Selected	Selected
❺ AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Added	Added	Added

❻ ❼

❽ No ICS Supplemental Guidance.

❾ Control Enhancement: (1) ICS Supplemental Guidance: Legacy ICS typically are typically configured with remote storage on a separate information system (e.g., the historian in the DMZ 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.

❿ Rationale for adding control to baseline:: 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.

Figure G-1 Detailed Overlay Control Specifications Illustrated

SP 800-53, Appendix F contains Supplemental Guidance for all Controls and Control Enhancements. ICS Supplemental Guidance in this overlay provides organizations with additional information on the application of the security controls and control enhancements in NIST SP 800-53, Appendix F to ICS and the environments in which these specialized systems operate. The ICS Supplemental Guidance also

provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). ICS Supplemental Guidance in this overlay adds to the original Supplemental Guidance in NIST SP 800-53, Appendix F.

ACCESS CONTROL – AC

Tailoring Considerations for Access Control Family

Before implementing controls in the AC family, consider the tradeoffs among security, privacy, latency, performance, throughput, and reliability. For example, the organization considers whether latency induced from the use of confidentiality and integrity mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the specific Access Control requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	Selected	Selected	Selected
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Selected	Selected
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*		Selected	Selected
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*		Selected	Selected
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Selected	Selected
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*			Selected
AC-2 (12)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Selected
AC-2 (13)	*ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*			Selected

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.

AC-3 ACCESS ENFORCEMENT

CNTL NO.	CONTROL NAME	CONTROL BASELINES

	Control Enhancement Name	LOW	MOD	HIGH
AC-3	**Access Enforcement**	Selected	Selected	Selected

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 ENFORCEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-4	**Information Flow Enforcement**		Selected	Selected

No ICS Supplemental Guidance.

AC-5 SEPARATION OF DUTIES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-5	**Separation of Duties**		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-6	**Least Privilege**		Selected	Selected
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*		Selected	Selected
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*		Selected	Selected
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*			Selected
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*		Selected	Selected
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*		Selected	Selected
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-7	**Unsuccessful Login Attempts**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-8	**System Use Notification**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-10	**Concurrent Session Control**			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-11	**Session Lock**		Selected	Selected
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-12	**Session Termination**		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-14	**Permitted Actions without Identification or Authentication**	Selected	Selected	Selected

No ICS Supplemental Guidance.

AC-17 REMOTE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-17	**Remote Access**	Selected	Selected	Selected
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*		Selected	Selected
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*		Selected	Selected
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*		Selected	Selected
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*		Selected	Selected

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). See Risk Management section TBD

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-18	**Wireless Access**	Selected	Selected	Selected
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*		Selected	Selected
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*			Selected
AC-18 (5)	*WIRELESS ACCESS | CONFINE WIRELESS COMMUNICATIONS*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-19	**Access Control for Mobile Devices**	Selected	Selected	Selected
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*		Selected	Selected

No ICS Supplemental Guidance.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-20	**Use of External Information Systems**	Selected	Selected	Selected
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*		Selected	Selected
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE MEDIA*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-21	**Collaboration and Information Sharing**	Added	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-22	**Publicly Accessible Content**	Selected	Selected	Selected

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).

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**	Selected	Selected	Selected

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 TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-2	**Security Awareness**	Selected	Selected	Selected
AT-2 (2)	*SECURITY AWARENESS | INSIDER THREAT*		Selected	Selected

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 ROLE-BASED SECURITY TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-3	**Role-Based Security Training**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-4	**Security Training Records**	Selected	Selected	Selected

No ICS Supplemental Guidance.

Tailoring Considerations for Audit Family

In general, audit information and audit tools are not present on legacy ICS, but on a separate information system (e.g., the historian). In situations where the ICS cannot support the specific Audit and Accountability requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**	Selected	Selected	Selected

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

AU-2 AUDIT EVENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-2	**Auditable Events**	Selected	Selected	Selected
AU-2 (3)	*AUDITABLE EVENTS | REVIEWS AND UPDATES*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-3	**Content of Audit Records**	Selected	Selected	Selected
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*		Selected	Selected
AU-3 (2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	**Audit Storage Capacity**	Selected	Selected	Selected
AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Added	Added	Added

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-5	**Response to Audit Processing Failures**	Selected	Selected	Selected
AU-5 (1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*			Selected
AU-5 (2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*			Selected

No ICS Supplemental Guidance.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-6	**Audit Review, Analysis, and Reporting**	Selected	Selected	Selected
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		Selected	Selected
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		Selected	Selected
AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*			Selected
AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-7	**Audit Reduction and Report Generation**		Selected	Selected
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		Selected	Selected

No ICS Supplemental Guidance.

Control Enhancement: (1) No ICS Supplemental Guidance.

AU-8 TIME STAMPS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-8	**Time Stamps**	Selected	Selected	Selected
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-9	**Protection of Audit Information**	Selected	Selected	Selected
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*			Selected
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*			Selected
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*		Selected	Selected

No ICS Supplemental Guidance.

AU-10 NON-REPUDIATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-10	**Non-repudiation**			Selected

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

AU-11 AUDIT RECORD RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-11	**Audit Record Retention**	Selected	Selected	Selected

No ICS Supplemental Guidance.

AU-12 AUDIT GENERATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-12	**Audit Generation**	Selected	Selected	Selected
AU-12 (1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*			Selected
AU-12 (3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*			Selected

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.

Tailoring Considerations for Security Assessment and Authorization Family

In situations where the ICS cannot support the specific Security Assessment and Authorization requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be **used in conjunction with the ICS Supplemental Guidance in this overlay, if any.**

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-2	**Security Assessments**	Selected	Selected	Selected
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		Selected	Selected
CA-2 (2)	*SECURITY ASSESSMENTS | TYPES OF ASSESSMENTS*			Selected

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 SYSTEM INTERCONNECTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-3	**Information System Connections**	Selected	Selected	Selected
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-5	**Plan of Action and Milestones**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CA-6 SECURITY AUTHORIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-6	**Security Authorization**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CA-7 CONTINUOUS MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-7	**Continuous Monitoring**	Selected	Selected	Selected
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-8	**Penetration Testing**			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-9	**Internal System Connections**	Selected	Selected	Selected

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.

Tailoring Considerations for Configuration Management Family

In situations where the ICS cannot be configured to restrict the use of unnecessary functions or cannot support the use of automated mechanisms to implement configuration management functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate. See Risk Management section TBD

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-2	**Baseline Configuration**	Selected	Selected	Selected
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		Selected	Selected
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*			Selected
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		Selected	Selected
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		Selected	Selected

No ICS Supplemental Guidance.

CM-3 CONFIGURATION CHANGE CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-3	**Configuration Change Control**		Selected	Selected
CM-3 (1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*			Selected
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		Selected	Selected

No ICS Supplemental Guidance.

CM-4 SECURITY IMPACT ANALYSIS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-4	**Security Impact Analysis**		Selected	Selected
CM-4 (1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*			Selected

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

Control Enhancement: (1) No ICS Supplemental Guidance.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-5	**Access Restrictions for Change**		Selected	Selected
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*			Selected
CM-5 (2)	*ACCESS RESTRICTIONS FOR CHANGE | AUDIT SYSTEM CHANGES*			Selected
CM-5 (3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*			Selected

No ICS Supplemental Guidance.

CM-6 CONFIGURATION SETTINGS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-6	**Configuration Settings**	Selected	Selected	Selected
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*			Selected
CM-6 (2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*			Selected

No ICS Supplemental Guidance.

CM-7 LEAST FUNCTIONALITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-7	**Least Functionality**	Selected	Selected	Selected
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	Added	Selected	Selected
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*		Selected	Selected
CM-7 (4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE*		Removed	
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE*		Added	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-8	**Information System Component Inventory**	Selected	Selected	Selected
CM-8 (1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		Selected	Selected
CM-8 (2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*			Selected
CM-8 (3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		Selected	Selected
CM-8 (4)	*INFORMATION SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION*			Selected
CM-8 (5)	*INFORMATION SYSTEM COMPONENT INVENTORY | ALL COMPONENTS WITHIN AUTHORIZATION BOUNDARY*		Selected	Selected

No ICS Supplemental Guidance.

CM-9 CONFIGURATION MANAGEMENT PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-9	**Configuration Management Plan**		Selected	Selected

No ICS Supplemental Guidance.

CM-10 SOFTWARE USAGE RESTRICTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-10	**Software Usage Restrictions**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CM-11 USER-INSTALLED SOFTWARE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-11	**User-Installed Software**	Selected	Selected	Selected

No ICS Supplemental Guidance.

Tailoring Considerations for Contingency Planning Family

ICS systems often contain a physical component at a fixed location. Such components may not be relocated logically. Some replacement components may not be readily available. Continuance of essential missions and business functions with little or no loss of operational continuity may not be possible. In situations where the organization cannot provide necessary essential services, support, or automated mechanisms during contingency operations, the organization provides nonautomated mechanisms or predetermined procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-2	**Contingency Plan**	Selected	Selected	Selected
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*		Selected	Selected
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*			Selected
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*		Selected	Selected
CP-2 (4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*			Selected
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*			Selected
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*		Selected	Selected

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.

Control Enhancement: (5, 8) No ICS Supplemental Guidance.

CP-3 CONTINGENCY TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-3	**Contingency Training**	Selected	Selected	Selected
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*			Selected

No ICS Supplemental Guidance.

CP-4 CONTINGENCY PLAN TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-4	**Contingency Plan Testing**	Selected	Selected	Selected
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		Selected	Selected
CP-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*			Selected

No ICS Supplemental Guidance.

CP-6 ALTERNATE STORAGE SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-6	**Alternate Storage Site**		Selected	Selected
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*		Selected	Selected
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*			Selected
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*		Selected	Selected

No ICS Supplemental Guidance.

CP-7 ALTERNATE PROCESSING SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-7	**Alternate Processing Site**		Selected	Selected
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*		Selected	Selected
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*		Selected	Selected
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*		Selected	Selected
CP-7 (4)	*ALTERNATE PROCESSING SITE | CONFIGURATION FOR USE*			Selected

No ICS Supplemental Guidance.

CP-8 TELECOMMUNICATIONS SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-8	**Telecommunications Services**		Selected	Selected
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*		Selected	Selected
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*		Selected	Selected
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*			Selected
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-9	**Information System Backup**	Selected	Selected	Selected
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*		Selected	Selected
CP-9 (2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*			Selected
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*			Selected
CP-9 (5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE SITE*			Selected

No ICS Supplemental Guidance.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-10	**Information System Recovery and Reconstitution**	Selected	Selected	Selected
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*		Selected	Selected
CP-10 (3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*		Selected	Selected
CP-10 (4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*			Selected
CP-10 (5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
CP-12	**Safe Mode**	Added	Added	Added

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.

Tailoring Considerations for Identification and Authentication Family

Before implementing controls in the IA family, consider the tradeoffs among security, privacy, latency, performance, and throughput. For example, the organization considers whether latency induced from the use of authentication mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the specific Identification and Authentication requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-1	**Security Identification and Authentication Policy and Procedures**	Selected	Selected	Selected

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)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-2	**Identification and Authentication (Organizational Users)**	Selected	Selected	Selected
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*	Selected	Selected	Selected
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*		Selected	Selected
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*		Selected	Selected
IA-2 (4)	*IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*			Selected
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*		Selected	Selected
IA-2 (9)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*			Selected
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*		Selected	Selected
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
IA-3	**Device Identification and Authentication**	Added	Selected	Selected
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*		Added	Added
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*		Added	Added

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-4	**Identifier Management**	Selected	Selected	Selected

No ICS Supplemental Guidance.

IA-5 AUTHENTICATOR MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-5	**Authenticator Management**	Selected	Selected	Selected
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	Selected	Selected	Selected
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*		Selected	Selected
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN PERSON REGISTRATION*		Selected	Selected
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-6	**Authenticator Feedback**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-7	**Cryptographic Module Authentication**	Selected	Selected	Selected

No ICS Supplemental Guidance.

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-8	**Identification and Authentication (Non-Organizational Users)**	Selected	Selected	Selected
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*	Selected	Selected	Selected
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*	Selected	Selected	Selected
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*	Selected	Selected	Selected
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*	Selected	Selected	Selected

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.

Tailoring Considerations for Incident Response Family

The automated mechanisms used to support the tracking of security incidents are typically not part of, or connected to, the ICS.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-2	**Incident Response Training**	Selected	Selected	Selected
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*			Selected
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*			Selected

No ICS Supplemental Guidance.

IR-3 INCIDENT RESPONSE TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-3	**Incident Response Testing**		Selected	Selected
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		Selected	Selected

No ICS Supplemental Guidance.

IR-4 INCIDENT HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-4	**Incident Handling**	Selected	Selected	Selected
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*		Selected	Selected
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*			Selected

No ICS Supplemental Guidance.

IR-5 INCIDENT MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-5	**Incident Monitoring**	Selected	Selected	Selected
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*			Selected

No ICS Supplemental Guidance.

IR-6 INCIDENT REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-6	**Incident Reporting**	Selected	Selected	Selected
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-7	**Incident Response Assistance**	Selected	Selected	Selected
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*		Selected	Selected

No ICS Supplemental Guidance.

IR-8 INCIDENT RESPONSE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-8	**Incident Response Plan**	Selected	Selected	Selected

No ICS Supplemental Guidance.

Tailoring Considerations for Maintenance Family

The automated mechanisms used to schedule, conduct, and document maintenance and repairs are not necessarily part of, or connected to, the ICS.

In situations where the ICS cannot support the specific Maintenance requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-1	**Maintenance Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-2	**Controlled Maintenance**	Selected	Selected	Selected
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*			Selected

No ICS Supplemental Guidance.

MA-3 MAINTENANCE TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-3	**Maintenance Tools**		Selected	Selected
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*		Selected	Selected
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*		Selected	Selected
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*			Selected

No ICS Supplemental Guidance.

MA-4 NONLOCAL MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-4	**Non-Local Maintenance**	Selected	Selected	Selected
MA-4 (2)	*NON-LOCAL MAINTENANCE | DOCUMENT NON-LOCAL MAINTENANCE*		Selected	Selected
MA-4 (3)	*NON-LOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-5	**Maintenance Personnel**	Selected	Selected	Selected
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*			Selected

No ICS Supplemental Guidance.

MA-6 TIMELY MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-6	**Timely Maintenance**		Selected	Selected

No ICS Supplemental Guidance.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-2	**Media Access**	Selected	Selected	Selected

No ICS Supplemental Guidance.

MP-3 MEDIA MARKING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-3	**Media Marking**		Selected	Selected

No ICS Supplemental Guidance.

MP-4 MEDIA STORAGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-4	**Media Storage**		Selected	Selected

No ICS Supplemental Guidance.

MP-5 MEDIA TRANSPORT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-5	**Media Transport**		Selected	Selected
MP-5 (4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*		Selected	Selected

No ICS Supplemental Guidance.

MP-6 MEDIA SANITIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-6	**Media Sanitization**	Selected	Selected	Selected
MP-6 (1)	*MEDIA SANITIZATION | TRACKING / DOCUMENTING / VERIFYING*			Selected
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*			Selected
MP-6 (3)	*MEDIA SANITIZATION | NON-DESTRUCTIVE TECHNIQUES*			Selected

No ICS Supplemental Guidance.

MP-7 MEDIA USE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-7	**Media Use**	Selected	Selected	Selected
MP-7 (1)	*MEDIA USE | ORGANIZATIONAL RESTRICTIONS*		Selected	Selected

No ICS Supplemental Guidance.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-2	**Physical Access Authorizations**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-3 PHYSICAL ACCESS CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-3	**Physical Access Control**	Selected	Selected	Selected
PE-3 (1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-4	**Access Control for Transmission Medium**		Selected	Selected

No ICS Supplemental Guidance.

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-5	**Access Control for Output Devices**		Selected	Selected

No ICS Supplemental Guidance.

PE-6 MONITORING PHYSICAL ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-6	**Monitoring Physical Access**	Selected	Selected	Selected
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		Selected	Selected
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		Added	Selected

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-8 VISITOR ACCESS RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-8	**Visitor Access Records**	Selected	Selected	Selected
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*			Selected

No ICS Supplemental Guidance.

PE-9 POWER EQUIPMENT AND CABLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-9	**Power Equipment and Cabling**		Selected	Selected
PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*		Added	Added

No ICS Supplemental Guidance.

Control Enhancement: (1) No ICS Supplemental Guidance.

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

PE-10 EMERGENCY SHUTOFF

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-10	**Emergency Shutoff**		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PE-11	**Emergency Power**	Added	Selected	Selected
PE-11 (1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*	Added	Added	Selected
PE-11 (2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*			Added

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) 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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-12	**Emergency Lighting**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-13 FIRE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-13	**Fire Protection**	Selected	Selected	Selected
PE-13 (1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*			Selected
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*			Selected
PE-13 (3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-14	**Temperature and Humidity Controls**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-15	**Water Damage Protection**	Selected	Selected	Selected
PE-15 (1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-16	**Delivery and Removal**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-17 ALTERNATE WORK SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-17	**Alternate Work Site**		Selected	Selected

No ICS Supplemental Guidance.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-18	**Location of Information System Components**			Selected

No ICS Supplemental Guidance.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PL-2	**System Security Plan**	Selected	Selected	Selected
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	Added	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-4	**Rules of Behavior**	Selected	Selected	Selected
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		Selected	Selected

No ICS Supplemental Guidance.

PL-7 SECURITY CONCEPT OF OPERATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
PL-7	**Security Concept of Operations**		Added	Added

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-8	**Information Security Architecture**		Selected	Selected

No ICS Supplemental Guidance.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**	Selected	Selected	Selected

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

PS-2 POSITION RISK DESIGNATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-2	**Position Risk Designation**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-3 PERSONNEL SCREENING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-3	**Personnel Screening**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-4 PERSONNEL TERMINATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-4	**Personnel Termination**	Selected	Selected	Selected
PS-4 (2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*			Selected

No ICS Supplemental Guidance.

PS-5 PERSONNEL TRANSFER

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-5	**Personnel Transfer**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-6 ACCESS AGREEMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-6	**Access Agreements**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-7 THIRD-PARTY PERSONNEL SECURITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-7	**Third-Party Personnel Security**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-8 PERSONNEL SANCTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-8	**Personnel Sanctions**	Selected	Selected	Selected

No ICS Supplemental Guidance.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-2	**Security Categorization**	Selected	Selected	Selected

No ICS Supplemental Guidance.

RA-3 RISK ASSESSMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-3	**Risk Assessment**	Selected	Selected	Selected

No ICS Supplemental Guidance.

RA-5 VULNERABILITY SCANNING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-5	**Vulnerability Scanning**	Selected	Selected	Selected
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		Selected	Selected
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		Selected	Selected
RA-5 (4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*			Selected
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		Selected	Selected

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.

SYSTEM AND SERVICES ACQUISITION

Tailoring Considerations for System and Services Acquisition Family

In situations where the ICS cannot support the specific System and Services Acquisition requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-2	**Allocation of Resources**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-3	**System Development Life Cycle**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-4 ACQUISITION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-4	**Acquisition Process**	Selected	Selected	Selected
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		Selected	Selected
SA-4 (2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		Selected	Selected
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		Selected	Selected
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-5	**Information System Documentation**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-8 SECURITY ENGINEERING PRINCIPLES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-8	**Security Engineering Principles**		Selected	Selected

No ICS Supplemental Guidance.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-9	**External Information System Services**	Selected	Selected	Selected
SA-9 (2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		Selected	Selected

No ICS Supplemental Guidance.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-10	**Developer Configuration Management**		Selected	Selected

No ICS Supplemental Guidance.

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-11	**Developer Security Testing and Evaluation**		Selected	Selected

No ICS Supplemental Guidance.

SA-12 SUPPLY CHAIN PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-12	**Supply Chain Protection**			Selected

No ICS Supplemental Guidance.

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**			Selected

No ICS Supplemental Guidance.

SA-16 DEVELOPER-PROVIDED TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-16	**Developer-Provided Training**			Selected

No ICS Supplemental Guidance.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-17	**Developer Security Architecture and Design**			Selected

No ICS Supplemental Guidance.

Tailoring Considerations for System and Communications Protection Family

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. While the legacy devices commonly found within ICS often lack direct support of cryptographic functions, compensating controls (e.g., encapsulations) may be used to meet the intent of the control.

In situations where the ICS cannot support the specific System and Communications Protection requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**	Selected	Selected	Selected

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

SC-2 APPLICATION PARTITIONING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-2	**Application Partitioning**		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-3	**Security Function Isolation**			Selected

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

SC-4 INFORMATION IN SHARED RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-4	**Information in Shared Resources**		Selected	Selected

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

SC-5 DENIAL OF SERVICE PROTECTION

CNTL NO.	CONTROL NAME	CONTROL BASELINES

	Control Enhancement Name	LOW	MOD	HIGH
SC-5	**Denial of Service Protection**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-7	**Boundary Protection**	Selected	Selected	Selected
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*		Selected	Selected
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*		Selected	Selected
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*		Selected	Selected
SC-7 (7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*		Selected	Selected
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*			Selected
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*		Added	**Selected**
SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*			Selected

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 CONFIDENTIALITY AND INTEGRITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-8	**Transmission Confidentiality and Integrity**		Selected	Selected
SC-8 (1)	**transmission confidentiality and integrity | cryptographic or alternate physical protection**		Selected	Selected

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-10 NETWORK DISCONNECT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-10	**Network Disconnect**		Selected	Selected

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

CNTL NO.	CONTROL NAME	CONTROL BASELINES

	Control Enhancement Name	LOW	MOD	HIGH
SC-12	**Cryptographic Key Establishment and Management**	Selected	Selected	Selected
SC-12 (1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*			Selected

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 CRYPTOGRAPHIC PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-13	**Cryptographic Protection**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SC-15 COLLABORATIVE COMPUTING DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-15	**Collaborative Computing Devices**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-17	**Public Key Infrastructure Certificates**		Selected	Selected

No ICS Supplemental Guidance.

SC-18 MOBILE CODE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-18	**Mobile Code**		Selected	Selected

No ICS Supplemental Guidance.

SC-19 VOICE OVER INTERNET PROTOCOL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-19	**Voice Over Internet Protocol**		Selected	Selected

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)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**	Selected	Selected	Selected

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 SERVICE (RECURSIVE OR CACHING RESOLVER)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	Selected	Selected	Selected

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 SESSION AUTHENTICITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-23	**Session Authenticity**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include auditing measures.

SC-24 FAIL IN KNOWN STATE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-24	**Fail in Known State**		Added	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-28	**Protection of Information at Rest**		Selected	Selected

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-39 PROCESS ISOLATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-39	**Process Isolation**	Selected	Selected	Selected

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

SC-41 PORT AND I/O DEVICE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SC-41	**Port and I/O Device Access**	Added	Added	Added

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.

Tailoring Considerations for System and Information Integrity Family

In situations where the ICS cannot support the specific System and Information Integrity requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**	Selected	Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-2	**Flaw Remediation**	Selected	Selected	Selected
SI-2 (1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*			Selected
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-3	**Malicious Code Protection**	Selected	Selected	Selected
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*		Selected	Selected
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-4	**Information System Monitoring**	Selected	Selected	Selected
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		Selected	Selected
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		Selected	Selected
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		Selected	Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-5	**Security Alerts, Advisories, and Directives**	Selected	Selected	Selected
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-6	**Security Function Verification**			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-7	**Software, Firmware, and Information Integrity**		Selected	Selected
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		Selected	Selected
SI-7 (2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*			Selected
SI-7 (5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*			Selected
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		Selected	Selected
SI-7 (14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*			Selected

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8	**Spam Protection**		Selected	Selected
SI-8 (1)	*SPAM PROTECTION | CENTRAL MANAGEMENT OF PROTECTION MECHANISMS*		Selected	Selected
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*		Selected	Selected

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-10 INFORMATION INPUT VALIDATION

CNTL NO.	CONTROL NAME	CONTROL BASELINES

	Control Enhancement Name	LOW	MOD	HIGH
SI-10	**Information Input Validation**		Selected	Selected

No ICS Supplemental Guidance.

SI-11 ERROR HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-11	**Error Handling**		Selected	Selected

No ICS Supplemental Guidance.

SI-12 INFORMATION HANDLING AND RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-12	**Information Handling and Retention**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SI-13 PREDICTABLE FAILURE PREVENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-13	**Predictable Failure Prevention**			Added

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.

Related controls: IR-5, IR-6, RA-5, SI-2, SI-5, SI-11.

Rationale for adding control to baseline: ICS are designed and built with certain boundary conditions, design parameters, and assumptions about their environment and mode of operation. ICS may run much longer than conventional systems, allowing latent flaws to become effective that are not manifest in other environments. For example, integer overflow might never occur in systems that are re-initialized more frequently than the occurrence of the overflow. Experience and forensic studies of anomalies and incidents in ICS can lead to identification of emergent properties that were previously unknown, unexpected, or unanticipated. Preventative and restorative

actions (e.g., re-starting the system or application) are prudent but may not be acceptable for operational reasons in ICS.

SI-16 MEMORY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-16	**Memory Protection**		Selected	Selected

No ICS Supplemental Guidance.

SI-17 FAIL-SAFE PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	SUPPLEMENTED CONTROL BASELINES		
		LOW	MOD	HIGH
SI-17	**Fail-Safe Procedures**	Added	Added	Added

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.

Characteristics of Organization-Wide Information Security Program Management Control Family

Organization-Wide Information Security Program Management Controls are deployed organization-wide supporting the information security program. They are not associated with security control baselines and are independent of any system impact level.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in SP 800-53, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PM-1 INFORMATION SECURITY PROGRAM PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-1	**Information Security Program Plan Policy and Procedures**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-2	**Senior Information Security Officer**

No ICS Supplemental Guidance.

PM-3 INFORMATION SECURITY RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-3	**Information Security Resources**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-4	**Plan of Action and Milestones Process**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-5	**Information System Inventory**

No ICS Supplemental Guidance.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-6	**Information Security Measures of Performance**

No ICS Supplemental Guidance.

PM-7 ENTERPRISE ARCHITECTURE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-7	**Enterprise Architecture**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-8	**Critical Infrastructure Plan**

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

References: Executive Order 13636– Improving Critical Infrastructure Cybersecurity, February 12, 2013

PM-9 RISK MANAGEMENT STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-9	**Risk Management Strategy**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-10	**Security Authorization Process**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-11	**Mission/Business Process Definition**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-12	**Insider Threat Program**

No ICS Supplemental Guidance.

PM-13 INFORMATION SECURITY WORKFORCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-13	**Information Security Workforce**

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

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-14	**Testing, Training, and Monitoring**

No ICS Supplemental Guidance.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-15	**Contacts with Security Groups and Associations**

No ICS Supplemental Guidance.

PM-16 THREAT AWARENESS PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-16	**Threat Awareness Program**

No ICS Supplemental Guidance.