Manufacturing Overlay

For additional questions, contact DoD CIO.
NIPR: OSD.RMFTAG-Secretariat@mail.mil

Last Updated: March 2024

Manufacturing Overlay

1. Purpose and Scope

This overlay was developed in partnership with the Defense Industrial Base (DIB) Cybersecurity (CS) Program, to develop a manufacturing overlay for control systems that is intended to complement (and further refine) their existing security control baselines. The Manufacturing Overlay Focus Group (FG), the driving body of this document, leveraged subject matter experts from across DoD, the Risk Management Framework (RMF) Technical Advisory Group (TAG), and industry partners from the DIB CS Program. As part of this effort, Manufacturing Overlay FG members provided expert domain knowledge on securing manufacturing systems and helped shape key concepts captured in supplemental control language. This resulted in guidance, for use during the Select Step, that complements and refines existing control baselines and addresses control specifications required to properly secure manufacturing systems.

The purpose of developing this document was to address security needs in DIB manufacturing systems and create a control overlay that produces tailored cybersecurity guidance. Overall, this produced a manufacturing systems control overlay that provides a standardized approach to securely implementing tailored controls for manufacturing systems within the DIB that complements the control baselines established in the DoD Control Systems Security Requirements Guide (SRG).

This overlay applies to manufacturing systems at a Low-Low-Moderate impact value for Confidentiality, Integrity, and Availability. Refer to the RMF Knowledge Service (KS) for additional information regarding the development, background, tailoring, and applicability of the Manufacturing Overlay. RMF KS: <https://rmfks.osd.mil/kslogin/>.

2. Authoritative References

The following documents were used to create this overlay:

- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020
- Committee on National Security Systems Instruction (CNSSI) 1253, *Categorization and Control Selection for National Security Systems*, July 2022
- DoD Instruction 8510.01, *RMF for DoD Systems*, July 2022
- DoD Control Systems Security Requirements Guide, Version 1, Release 1, July 2021
- NIST SP 800-82, Revision 3, *Guide to Operational Technology (OT) Security*, September 2023

3. Overlay Characteristics

This Manufacturing Overlay applies to systems, including control systems of any type, Internet of Things devices, sensors and technologies supporting DoD manufacturing processes. Manufacturing processes may include (list is not exhaustive):

- Additive Manufacturing
- Batch Manufacturing
- Continuous Manufacturing
- Electronic and mechanical parts assembly
- Discrete-based Manufacturing

This overlay provides tailored controls to the distinct security requirements of manufacturing systems and processes while remaining useful to as many types of manufacturing systems as possible. While manufacturing systems exist in a multitude of environments with varying levels of sensitivity, this overlay is intended to provide system owners and authorizing officials with preliminary security controls for DoD control systems supporting manufacturing processes.

Users should reference the RMF KS for more background information on this overlay: https://rmfks.osd.mil/rmf/RMFforDoDTech/ControlSystems/Pages/ManufacturingSystems.aspx

Each DoD organization retains the autonomy to determine its own risk tolerance for manufacturing systems using the policy requirements articulated by the DoDI 8500 series, guidelines found on the RMF KS, and the parameters of organization-specific cybersecurity programs. Organizations can tailor controls in or out of the established baseline depending on their requisite security requirements, risk tolerances, and system capabilities.

Additional security considerations beyond the scope of this overlay may be required for manufacturing systems operating in more sensitive environments; and future guidance will address systems at higher criticality levels. Compensating controls are especially important because the operating environments of manufacturing systems are different than what is assumed in the baselines.

Organizations should use the Manufacturing Overlay as appropriate based on their requisite security requirements for a particular system or mission need. As in all risk-based management, organizations must analyze their manufacturing systems to determine how this overlay will fit their operational environment.

4. Applicability

Use the following questions to determine the applicability of the Manufacturing Overlay:

1. Is the system being developed for or used in any DIB or other DoD manufacturing functions? If yes, system owners should apply this overlay.
2. Is the system being developed for or used as a component in a larger manufacturing system? If yes, utilize key cybersecurity principles from this overlay to assess the system component.
3. System owners should consult the DoD Control Systems SRG to inform organizational cybersecurity activities for all control systems in the DoD. The DoD Control Systems SRG also addresses high criticality mission objectives; system owners should consider this criticality when selecting controls to mitigate cybersecurity risks. Refer to tables in the DoD Control Systems SRG that map security requirements to specific controls.

5. Summary of Control Specifications

The table below contains a summary of the control specifications that apply in this overlay. The symbols used in the table are as follows:

- The letter "X" indicates there is supplemental guidance, including specific tailoring guidance if applicable, is available for the control.
- Controls with a ~~strikethrough~~ indicate the control has been removed from this overlay.

Control ID	Control Name	Supplemental Guidance
AC-1	(Access Control) Policy and Procedures	
AC-2	Account Management	
AC-2(4)	Account Management | Automated Audit Actions	X
AC-2(5)	Account Management | Inactivity Logout	X
AC-2(7)	Account Management | Privileged User Accounts	
AC-2(9)	Account Management | Restrictions On Use of Shared and Group Accounts	
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	X
AC-3	Access Enforcement	
AC-3(4)	Access Enforcement | Discretionary Access Control	
AC-5	Separation of Duties	
AC-6	Least Privilege	
AC-6(1)	Least Privilege | Authorize Access to Security Functions	X
AC-6(5)	Least Privilege | Privileged Accounts	
AC-6(7)	Least Privilege | Review of User Privileges	
AC-6(8)	Least Privilege | Privilege Levels for Code Execution	
AC-6(9)	Least Privilege | Log Use of Privileged Functions	
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	
AC-7	Unsuccessful Logon Attempts	
AC-8	System Use Notification	X
AC-10	Concurrent Session Control	X
AC-11	Device Lock	
AC-11(1)	Device Lock | Pattern-Hiding Displays	
AC-14	Permitted Actions Without Identification or Authentication	
AC-17	Remote Access	
AC-17(1)	Remote Access | Monitoring and Control	
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	
AC-17(3)	Remote Access | Managed Access Control Points	
AC-17(4)	Remote Access | Privileged Commands and Access	
AC-17(6)	Remote Access | Protection of Mechanism Information	
AC-17(9)	Remote Access | Disconnect or Disable Access	

Control ID	Control Name	Supplemental Guidance
AC-18	Wireless Access	
AC-18(1)	Wireless Access | Authentication and Encryption	
AC-18(3)	Wireless Access | Disable Wireless Networking	
AC-18(4)	Wireless Access | Restrict Configurations By Users	
AC-19	Access Control for Mobile Devices	
AC-20	Use of External Systems	
AC-20(1)	Use of External Systems | Limits On Authorized Use	
AC-20(2)	Use of External Systems | Portable Storage Devices – Restricted Use	
AC-20(3)	Use of External Systems | Non-Organizationally Owned Systems — Restricted Use	
AC-22	Publicly Accessible Content	X
AT-1	(Awareness and Training) Policy and Procedures	
AT-2	Literacy Training and Awareness	
AT-2(2)	Literacy Training and Awareness | Insider Threat	
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior	
AT-3	Role-Based Training	
AT-3(2)	Role-Based Training | Physical Security Controls	
AT-4	Training Records	
AU-1	(Audit and Accountability) Policy and Procedures	
AU-2	Event Logging	X
AU-3	Content of Audit Records	
AU-3(1)	Content of Audit Records | Additional Audit Information	
AU-4	Audit Log Storage Capacity	X
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	X
AU-5	Response to Audit Logging Process Failures	
AU-6	Audit Record Review, Analysis, and Reporting	X
AU-6(1)	Audit Record Review, Analysis, and Reporting | Automated Process Integration	
AU-6(3)	Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories	
AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	
AU-8	Time Stamps	
AU-9	Protection of Audit Information	
AU-9(4)	Protection of Audit Information | Access By Subset of Privileged Users	
AU-11	Audit Record Retention	
AU-11(1)	Audit Record Retention | Long-Term Retrieval Capability	X
AU-12	Audit Record Generation	

Control ID	Control Name	Supplemental Guidance
AU-12(1)	Audit Record Generation | System-Wide and Time-Correlated Audit Trail	X
AU-12(3)	Audit Record Generation | Changes By Authorized Individuals	X
AU-14	Session Audit	X
AU-14(1)	System Start-Up	X
AU-14(3)	Session Audit | Remote Viewing and Listening	
CA-1	(Assessment, Authorization, and Monitoring) Policies and Procedures	
CA-2	Control Assessments	
CA-2(1)	Control Assessments | Independent Assessors	
CA-3	Information Exchange	X
CA-5	Plan of Action and Milestones	
CA-6	Authorization	
CA-7	Continuous Monitoring	
CA-7(1)	Continuous Monitoring | Independent Assessment	
CA-9	Internal System Connections	X
CM-1	(Configuration Management) Policy and Procedures	
CM-2	Baseline Configuration	
CM-2(7)	Baseline Configuration | Configure Systems and Components for High-Risk Areas	
CM-3	Configuration Change Control	
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	X
CM-3(6)	Configuration Change Control | Cryptography Management	
CM-4	Impact Analyses	
CM-5	Access Restrictions for Change	X
CM-5(5)	Access Restrictions for Change | Privilege Limitation for Production and Operation	
CM-5(6)	Access Restrictions for Change | Limit Library Privileges	
CM-6	Configuration Settings	
CM-7	Least Functionality	
CM-7(1)	Least Functionality | Periodic Review	
CM-7(2)	Least Functionality | Prevent Program Execution	
CM-7(3)	Least Functionality | Registration Compliance	
CM-7(5)	Least Functionality | Authorized Software -- Allow by Exception	
CM-7(8)	Least Functionality | Binary or Machine Executable Code	
CM-8	System Component Inventory	
CM-8(2)	System Component Inventory | Automated Maintenance	
CM-8(3)	System Component Inventory | Automated Unauthorized Component Detection	

Control ID	Control Name	Supplemental Guidance
CM-9	Configuration Management Plan	
CM-10	Software Usage Restrictions	
CM-10(1)	Software Usage Restrictions | Open Source Software	
CM-11	User-Installed Software	
CM-11(2)	User-Installed Software | Software Installation With Privileged Status	
CP-1	(Contingency Planning) Policy and Procedures	
CP-2	Contingency Plan	
CP-2(1)	Contingency Plan | Coordinate With Related Plans	
CP-2(3)	Contingency Plan | Resume Mission and Business Functions	
CP-2(8)	Contingency Plan | Identify Critical Assets	
CP-3	Contingency Training	
CP-4	Contingency Plan Testing	
CP-4(1)	Contingency Plan Testing | Coordinate With Related Plans	
CP-6	Alternate Storage Site	
CP-6(1)	Alternate Storage Site | Separation From Primary Site	
CP-6(3)	Alternate Storage Site | Accessibility	
CP-7	Alternate Processing Site	X
CP-7(1)	Alternate Processing Site | Separation From Primary Site	
CP-7(2)	Alternate Processing Site | Accessibility	
CP-7(3)	Alternate Processing Site | Priority of Service	
CP-8	Telecommunications Services	X
CP-8(1)	Telecommunications Services | Priority of Service Provisions	
CP-8(2)	Telecommunications Services | Single Points of Failure	
CP-9	System Backup	
CP-9(1)	System Backup | Testing for Reliability and Integrity	
CP-9(5)	System Backup | Transfer to Alternate Storage Site	
CP-10	System Recovery and Reconstitution	X
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	
IA-1	(Identification and Authentication) Policy and Procedures	
IA-2	Identification and Authentication (Organizational Users)	
IA-2(1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	
IA-2(2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	
IA-2(5)	Identification and Authentication (Organizational Users) | Individual Authentication With Group Authentication	
IA-2(6)	Literacy Training and Awareness | Cyber Threat Environment	
IA-2(8)	Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant	
IA-2(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	X

Control ID	Control Name	Supplemental Guidance
IA-3	Device Identification and Authentication	
IA-4	Identifier Management	
IA-5	Authenticator Management	
IA-5(1)	Authenticator Management | Password-Based Authentication	
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators	
IA-5(8)	Authenticator Management | Multiple System Accounts	
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	X
IA-6	Authenticator Feedback	
IA-7	Cryptographic Module Authentication	X
IA-8	Identification and Authentication (Non-Organizational Users)	X
IA-8(1)	Identification and Authentication (Non-Organizational Users) |Acceptance of PIV Credentials From Other Agencies	X
IA-8(2)	Identification and Authentication (Non-Organizational Users) |Acceptance of External Party Credentials	
IA-8(4)	Identification and Authentication (Non-Organizational Users) |	
IR-1	(Incident Response) Policy and Procedures	
IR-2	Incident Response Training	
IR-3	Incident Response Testing	
IR-3(2)	Incident Response Testing | Coordination With Related Plans	
IR-4	Incident Handling	X
IR-4(1)	Incident Handling | Automated Incident Handling Processes	
IR-4(3)	Incident Handling | Continuity of Operations	
IR-4(4)	Incident Handling | Information Correlation	
IR-4(6)	Incident Handling | Insider Threats — Specific Capabilities	
IR-4(7)	Incident Handling | Insider Threats — Intra-Organization Coordination	
IR-4(8)	Incident Handling | Correlation With External Organizations	
IR-4(11)	Incident Handling | Integrated Incident Response Team	
IR-5	Incident Monitoring	
IR-6	Incident Reporting	X
IR-6(1)	Incident Reporting | Automated Reporting	X
IR-6(2)	Incident Reporting | Vulnerabilities Related to Incidents	
IR-6(3)	Incident Reporting | Supply Chain Coordination	
IR-7	Incident Response Assistance	
IR-7(1)	Incident Response Assistance | Automation Support for Availability of Information and Support	
IR-7(2)	Incident Response Assistance | Coordination With External Providers	
IR-8	Incident Response Plan	

Control ID	Control Name	Supplemental Guidance
IR-9	Information Spillage Response	
IR-9(2)	Information Spillage Response | Training	
MA-1	(Maintenance) Policy and Procedures	
MA-2	Controlled Maintenance	
MA-3	Maintenance Tools	
MA-3(2)	Maintenance Tools | Inspect Media	
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	
MA-4	Nonlocal Maintenance	X
MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	
MA-4(6)	Nonlocal Maintenance | Cryptographic Protection	
MA-4(7)	Nonlocal Maintenance | Disconnect Verification	
MA-5	Maintenance Personnel	
MA-6	Timely Maintenance	
MP-1	(Media Protection) Policy and Procedures	
MP-2	Media Access	
MP-6	Media Sanitization	
MP-7	Media Use	
PE-1	(Physical and Environmental Protection) Policy and Procedures	
PE-2	Physical Access Authorizations	
PE-3	Physical Access Control	
PE-3(1)	Physical Access Control | System Access	
PE-6	Monitoring Physical Access	
PE-6(1)	Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment	
PE-8	Visitor Access Records	
PE-9	Power Equipment and Cabling	
PE-10	Emergency Shutoff	
PE-11	Emergency Power	
PE-12	Emergency Lighting	
PE-13	Fire Protection	
PE-13(2)	Fire Protection | Suppression Systems – Automatic Activation and Notification	
PE-14	Environmental Controls	
PE-15	Water Damage Protection	
PE-16	Delivery and Removal	
PE-17	Alternate Work Site	
PL-1	(Planning) Policy and Procedures	
PL-2	System Security and Privacy Plans	
PL-4	Rules of Behavior	
PL-8	Security and Privacy Architectures	
PL-8(1)	Security and Privacy Architectures | Defense-In-Depth	

Control ID	Control Name	Supplemental Guidance
PL-9	Central Management	X
PM-1	Information Security Program Plan	
PM-2	Information Security Program Role	
PM-3	Information Security and Privacy Resources	
PM-4	Plan of Action and Milestones Process	
PM-5	System Inventory	
PM-6	Measures of Performance	
PM-7	Enterprise Architecture	
PM-8	Critical Infrastructure Plan	
PM-9	Risk Management Strategy	
PM-10	Authorization Process	
PM-11	Mission and Business Process Definition	
PM-12	Insider Threat Program	
PM-13	Security and Privacy Workforce	
PM-14	Testing, Training, and Monitoring	
PM-15	Security and Privacy Groups and Associations	
PM-16	Threat Awareness Program	
PS-1	(Personnel Security) Policy and Procedures	
PS-2	Position Risk Designation	
PS-3	Personnel Screening	
PS-4	Personnel Termination	
PS-4(1)	Personnel Termination | Post-Employment Requirements	
PS-5	Personnel Transfer	
PS-6	Access Agreements	
PS-6(3)	Access Agreements | Post-Employment Requirements	
PS-7	External Personnel Security	
PS-8	Personnel Sanctions	
PT-1	(Personally Identifiable Information Processing and Transparency) Policy and Procedures	
PT-2	Authority to Process Personally Identifiable Information	
RA-1	(Risk Assessment) Policy and Procedures	
RA-2	Security Categorization	
RA-3	Risk Assessment	
RA-3(1)	Risk Assessment | Supply Chain Risk Assessment	
RA-5	Vulnerability Monitoring and Scanning	X
RA-5(2)	Vulnerability Monitoring and Scanning | Update Vulnerabilities to be Scanned	
RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	X
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	
SA-1	(System and Services Acquisition) Policy and Procedures	
SA-2	Allocation of Resources	

Control ID	Control Name	Supplemental Guidance
SA-3	System Development Life Cycle	
SA-3(2)	System Development Life Cycle | Use of Live or Operational Data	
SA-4	Acquisition Process	
SA-4(1)	Acquisition Process | Functional Properties of Controls	
SA-4(2)	Acquisition Process | Design and Implementation Information for Controls	
SA-4(7)	Acquisition Process | NIAP-Approved Protection Profiles	
SA-4(9)	Acquisition Process | Functions, Ports, Protocols, and Services In Use	
SA-4(10)	Acquisition Process | Use of Approved PIV Products	
SA-5	System Documentation	
SA-8	Security and Privacy Engineering Principles	
SA-9	External System Services	
SA-9(1)	External System Services | Risk Assessments and Organizational Approvals	
SA-9(2)	External System Services | Identification of Functions, Ports, Protocols, and Services	
SA-10	Developer Configuration Management	
SA-10(1)	Developer Configuration Management | Software and Firmware Integrity Verification	
SA-11	Developer Testing and Evaluation	
SA-15	Development Process, Standards, and Tools	
SC-1	(System and Communications Protection) Policy and Procedures	
SC-5	Denial of Service Protection	
SC-5(1)	Denial of Service Protection | Restrict Ability to Attack Other Systems	
SC-5(2)	Denial of Service Protection | Capacity, Bandwidth, and Redundancy	
SC-5(3)	Denial of Service Protection | Detection and Monitoring	
SC-7	Boundary Protection	
SC-7(3)	Boundary Protection | Access Points	
SC-7(4)	Boundary Protection | External Telecommunications Services	
SC-7(5)	Boundary Protection | Deny By Default — Allow By Exception	
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic	
SC-7(10)	Boundary Protection | Prevent Exfiltration	

Control ID	Control Name	Supplemental Guidance
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic	
SC-7(12)	Boundary Protection | Host-Based Protection	
SC-7(13)	Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components	
SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections	
SC-7(25)	Boundary Protection | Unclassified National Security System Connections	
SC-8	Transmission Confidentiality and Integrity	
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	
SC-12	Cryptographic Key Establishment and Management	
SC-13	Cryptographic Protection	
SC-15	Collaborative Computing Devices and Applications	
SC-17	Public Key Infrastructure Certificates	
SC-18	Mobile Code	
SC-18(1)	Identify Unacceptable Code and Take Corrective Actions	
SC-18(2)	Acquisition, Development, and Use	
SC-18(3)	Prevent Downloading and Execution	
SC-18(4)	Prevent Automatic Execution	
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	X
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	X
SC-23	Session Authenticity	
SC-23(1)	Session Authenticity | Invalidate Session Identifiers At Logout	
SC-23(3)	Session Authenticity | Unique System-Generated Session Identifiers	
SC-23(5)	Session Authenticity | Allowed Certificate Authorities	
SC-28	Protection of Information At Rest	
SC-28(1)	Protection of Information At Rest | Cryptographic Protection	
SC-38	Operations Security	
SC-39	Process Isolation	
SC-45(1)	System Time Synchronization | Synchronization with Authoritative Time Source	
SI-1	(System and Information Integrity) Policy and Procedures	
SI-2	Flaw Remediation	X
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status	

Control ID	Control Name	Supplemental Guidance
SI-2(3)	Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions	
SI-2(6)	Flaw Remediation | Removal of Previous Versions of Software and Firmware	
SI-3	Malicious Code Protection	
SI-3(10)	Malicious Code Protection | Malicious Code Analysis	
SI-4	System Monitoring	
SI-4(1)	System Monitoring | System-Wide Intrusion Detection System	
SI-4(2)	System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis	
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	
SI-4(5)	System Monitoring | System-Generated Alerts	
SI-4(10)	System Monitoring | Visibility of Encrypted Communications	
SI-4(11)	System Monitoring | Analyze Communications Traffic Anomalies	
SI-4(12)	System Monitoring | Automated Organization-Generated Alerts	
SI-4(14)	System Monitoring | Wireless Intrusion Detection	X
SI-4(15)	System Monitoring | Wireless to Wireline Communications	X
SI-4(16)	System Monitoring | Correlate Monitoring Information	
SI-4(19)	System Monitoring | Risk for Individuals	
SI-4(20)	System Monitoring | Privileged Users	
SI-4(22)	System Monitoring | Unauthorized Network Services	
SI-4(23)	System Monitoring | Host-Based Devices	
SI-5	Security Alerts, Advisories, and Directives	
SI-8	Spam Protection	X
~~SI-8(2)~~	~~Spam Protection | Automatic Updates~~	X
SI-10	Information Input Validation	
SI-11	Error Handling	
SI-12	Information Management and Retention	
SR-1	(Supply Chain Risk Management) Policy and Procedures	
SR-2	Supply Chain Risk Management Plan	
SR-2(1)	Supply Chain Risk Management Plan | Establish SCRM Team	
SR-3	Supply Chain Controls and Processes	
SR-5	Acquisition Strategies, Tools, and Methods	
SR-5(1)	Acquisition Strategies, Tools, and Methods | Adequate Supply	
SR-6	Supplier Assessments and Reviews	
SR-8	Notification Agreements	
SR-10	Inspection of Systems or Components	
SR-11	Component Authenticity	

Control ID	Control Name	Supplemental Guidance
SR-11(1)	Component Authenticity | Anti-counterfeit Training	
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	
SR-12	Component Disposal	

6. Supplemental Guidance

During the development of this Manufacturing Overlay, 42 controls were identified as requiring additional supplemental guidance. These controls include:

- AC-2(4)
- AC-2(5)
- AC-2(12)
- AC-6(1)
- AC-8
- AC-10
- AC-22
- AU-2
- AU-4
- AU-4(1)
- AU-6
- AU-11(1)
- AU-12(1)
- AU-12(3)
- AU-14
- AU-14(1)
- CA-3
- CA-9
- CM-3(4)
- CM-5
- CP-7
- CP-8
- CP-10
- IA-2(12)
- IA-5(13)
- IA-7
- IA-8
- IA-8(1)
- IR-4
- IR-6
- IR-6(1)
- MA-4
- PL-9
- RA-5
- RA-5(4)
- SC-20
- SC-22
- SI-2
- SI-4(14)
- SI-4(15)
- SI-8
- ~~SI-8(2)~~

The specific supplemental guidance for each of these controls can be found in Table 2, Manufacturing Supplemental Guidance.

Table 2, Manufacturing Supplemental Guidance

Control ID	Control Name	Supplemental Guidance
AC-2(4)	Account Management | Automated Audit Actions	The system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies the system administrator and Information Systems Security Officer (ISSO). Many manufacturing systems do not possess the technological capability to satisfy this control. If the manufacturing system of interest is connected to a system with automated audit capabilities, this control should be implemented; however, automated audit actions may not be feasible for manufacturing systems that do not interact with a system possessing these capabilities. As such, this control may not be applicable in particular scenarios.

Control ID	Control Name	Supplemental Guidance
		Related Controls: AU-2, AU-6
AC-2(5)	Account Management | Inactivity Logout	The organization requires that users log out when at the end of the users' standard work period unless otherwise defined in formal organizational policy. Given the unique uptime requirements of manufacturing systems, system operators may have extended periods where they are logged on in order to execute lengthy manufacturing processes. As such, organizations should carefully consider the operational requirements of their manufacturing systems. Policy addressing logout requirements necessary for maintaining operational continuity in the manufacturing system environment should be defined by the organization. Related Controls: AC-11
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	Organizations should monitor manufacturing system accounts for atypical usage and report atypical usage of manufacturing system accounts to the ISSO, where feasible. Many manufacturing systems do not possess the technological capability to satisfy this control. As such, organizations must consider the applicability of this control based on the monitoring capabilities associated with the manufacturing system environment. Related Controls: AU-6, AU-7, CA-7, IR-8, SI-4
AC-6(1)	Least Privilege | Authorize Access to Security Functions	Security functions include establishing system accounts; configuring access authorizations (i.e., permissions, privileges), configuring settings for events to be audited, and establishing intrusion detection parameters. Organizations should carefully consider the security functions that their manufacturing systems possess. Organizations should also consider the system account types associated with their manufacturing systems. This can vary from multiple user accounts with differing levels of access to one shared account with one password and identical privileges. As such, it is critical that organizations carefully consider the security functions their systems possess when implementing this control. Related Controls: AC-17, AC-18, AC-19, AU-9, PE-2
AC-8	System Use Notification	Many OT systems must remain in continuous operation, and system use notification may not be supported or effective. Example compensating controls include posting

Control ID	Control Name	Supplemental Guidance
		physical notices in OT facilities or providing recurring training on system use prior to permitting access.
AC-10	Concurrent Session Control	Many manufacturing systems have operating systems that do not have the capability for concurrent sessions. This control should only be implemented where feasible. This control addresses concurrent sessions for system accounts and does not address concurrent sessions by single users via multiple system accounts. Related Controls: SC-23
AC-22	Publicly Accessible Content	This control should be implemented in manufacturing systems that have the capability to push information to a publicly accessible system. Organizations should carefully consider the risk associated with making information publicly accessible. This control is not applicable to systems lacking this capability. Related Controls: AC-3, AT-2, AT-3, AU-13
AU-2	Event Logging	Organizations should carefully consider the auditing capabilities of their manufacturing systems when establishing event logging practices. Examples of "events" include password changes; failed logons or failed accesses related to systems; security or privacy attribute changes; administrative privilege usage; PIV credential usage; data action changes; query parameters; or external credential usage. Manufacturing systems vary significantly in complexity and technical capability. As such, organizations should determine the types of events that need to be logged to ensure mission success in the manufacturing system environment. Related Controls: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11
AU-4	Audit Log Storage Capacity	Many manufacturing systems do not have the capability to specify log storage capacity. Organizations should consider the types of audit logging to be performed and the audit log processing requirements when allocating audit log storage capacity. Allocating sufficient audit log storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of audit logging

Control ID	Control Name	Supplemental Guidance
		capability. In instances where a data historian exists on the manufacturing system and logs can be pulled or the system utilizes storage area networks (SAN) / network-attached storage (NAS) solutions, organizations should implement this control. If the manufacturing system does not have the function to specify log storage capacity, this control is not applicable. Related Controls: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4
AU-4(1)	Audit Log Storage Capacity | Transfer to Alternate Storage	Similar to control AU-4, some manufacturing systems utilize SAN/NAS solutions, data historians, or other data recording capabilities. If so, organizations should transfer audit logs to a different system, system component, or media other than the system or system component conducting the logging. This control is not applicable to manufacturing systems that lack the ability to transfer audit log information to an alternate location. Related Controls: None
AU-6	Audit Record Review, Analysis, and Reporting	Organizations should consider the unique auditing capabilities of their manufacturing systems. If the systems of interest do not possess the functionality to adjust the level of audit review, analysis, and reporting, this control is not applicable. Related Controls: AC-2, AC-3, AC-5, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SA-8, SC-7, SI-3, SI-4, SI-7.
AU-11(1)	Audit Record Retention | Long-Term Retrieval Capability	Organizations should consider the auditing capabilities of their manufacturing systems. Some manufacturing systems utilize SAN/NAS solutions and have audit log transfer capabilities, allowing for long-term retrieval of audit logs. Other systems have the capability to prevent audit log data from being overwritten until the information is transferred to an alternate storage location. Regarding systems with these capabilities, organizations should define the length of time that audit records need to be retained so they can be retrieved. This control is not applicable to manufacturing systems that lack functionality to retain audit records or transfer them to a more permanent medium.

Control ID	Control Name	Supplemental Guidance
		Related Controls: None.
AU-12(1)	Audit Record Generation | System-Wide and Time-Correlated Audit Trail	Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. This control can be very critical for time-based troubleshooting purposes. For manufacturing systems with network connectivity and the capability to pull time stamps from a Network Time Protocol (NTP) server, organizations should ensure this control is implemented in accordance with the time tracking tolerance defined in AU-8. Organizations should carefully consider the auditing capabilities of their manufacturing systems. Particularly with embedded systems and air-gapped systems, accessible time services may not be technically feasible. As such, this guidance is included based on the time-reporting and audit capabilities of the system and is not applicable to systems lacking this functionality. Related Controls: AU-8, SC-45
AU-12(3)	Audit Record Generation | Changes By Authorized Individuals	Manufacturing systems' unique uptime requirements warrant careful considerations in altering logs for reporting. Permitting authorized individuals to make changes to system logging enables organizations to extend or limit logging as necessary to meet organizational requirements. Logging that is limited to conserve system resources may be extended (either temporarily or permanently) to address certain threat situations. In addition, logging may be limited to a specific set of event types to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which logging actions are changed, for example, near real time, within minutes, or within hours. Regarding manufacturing systems, particular incidents may require a system administrator to view and/or alter logs for reporting. Organizations should ensure that any changes would be processed by a change-control board or another change management process, so all necessary parties are aware of any changes that are made. Related Controls: AC-3
AU-14	Session Audit	Session audits can include, but are not limited to, monitoring keystrokes, tracking websites visited, and recording transfers of information or files. To ensure they

Control ID	Control Name	Supplemental Guidance
		are complying with applicable federal laws, Executive Orders, directives, policies, regulations, or standards, organizations should consult legal counsel while developing, integrating, and using session auditing activities. Particularly for manufacturing systems, there is always risk of system failure causing physical injury. This control can be critical in legal situations where authorities would want to conduct a session audit to determine negligence. In the absence of an ability to execute a full session audit, organizations should implement the control to the maximum extent that is technically feasible. Organizations must maintain accurate audit logs as well as complete and detailed operator schedules to allow, to the greatest extent possible, organizations the ability to "triangulate" the session usage to the operator on duty. Related Controls: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12
AU-14(1)	System Start-Up	Where feasible, manufacturing systems should initiate user session audits upon system start up to provide a full picture of user activity. In the absence of this system capability, information should be captured from the beginning of a users' session on the system. Specific policy to capture the entire user session for audit should be defined by the organization. Related Controls: None
CA-3	Information Exchange	Organizations should develop connection and boundary limitations at the system level in consultation with appropriate parties (e.g., Authorizing Official, Information System Security Manager, Cyber Security Service Provider). Organizations should document and define system interconnections in organizational security policies. Organizations should also carefully consider the sensitivity and risks associated with their system environment when defining system interconnections. Related control: AC-4, AC-20, AU-16, CA-6, IA-3, IR-4, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12
CA-9	Internal System Connections	Internal system connections are connections between organizational systems and separate constituent system components (i.e., connections between components that are part of the same system). Organizations operating

Control ID	Control Name	Supplemental Guidance
		manufacturing systems should carefully consider the technical capabilities and complexity of each system component in the manufacturing system environment. Organizations should be aware of data flow and connectivity of each system component to see if components have external connectivity that could result in additional vulnerabilities. The continued need for an internal system connection should be reviewed from the perspective of whether the connection provides support for organizational missions or business functions. All connections within the boundary should be documented. Organizations may exclude this control if it does not apply to their system. Related Controls: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12
CM-3(4)	Configuration Change Control | Security and Privacy Representatives	Information security representatives can include senior agency information security officers, information system security officers, or information system security managers. It is important to involve personnel with information security expertise in this process because changes to system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid negative consequences that could ultimately affect the security state of organizational manufacturing systems. This is particularly important in manufacturing system environments where unintended consequences from system configuration changes could result in physical harm on top of system failure. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3. In the absence of a senior agency official, organizations can define the appropriate security representative based on their technically qualified personnel, mission need, system specific qualifications, and organizational availability. Related Controls: None.
CM-5	Access Restrictions for Change	Changes to the hardware, software, or firmware components of systems or the operational procedures related to the system, can potentially have significant effects on the security of the systems. Therefore, organizations permit only qualified and authorized

Control ID	Control Name	Supplemental Guidance
		individuals to access systems for purposes of initiating changes. Access restrictions include physical and logical access controls (see AC-3 and PE-3), software libraries, workflow automation, media libraries, abstract layers (i.e., changes implemented into external interfaces rather than directly into systems), and change windows (i.e., changes occur only during specified times). Organizations operating manufacturing systems must carefully consider access restrictions for configuration changes because negative consequences from unauthorized or unintended changes could significantly impact continuity of operations and even lead to physical harm. Related Controls: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10
CP-7	Alternate Processing Site	Many site-wide supervisory or optimization servers (i.e., Level 3 and above of the Purdue model) can be supported from an alternate processing site. It is likely not feasible for control systems or field devices, such as sensors or final elements (i.e., Level 1 and 0 of the Purdue model), to be made available from an alternate processing site. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13
CP-8	Telecommunications Services	Quality of service factors for OT include latency and throughput. Related controls: CP-2, CP-6, CP-7, CP-11, SC-7
CP-10	System Recovery and Reconstitution	Reconstitution of the OT includes considering whether system state variables should be restored to initial values or the 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). Related controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13
IA-2(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	The acceptance of PIV credentials is only required for federal organizations, as defined by OMB Memorandum M-19-17. Nonfederal organizations should refer to IA-2(1)(2) for guidance on multi-factor authentication credentials. Furthermore, many OT systems do not have the ability to

Control ID	**Control Name**	**Supplemental Guidance**
		accept PIV credentials and will require compensating controls. Related controls: None.
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators	Authenticators include passwords, cryptographic devices, one-time password devices, and key cards. If cached authentication information is out-of-date, the validity of the authentication information may be questionable. User identity must be confirmed prior to any system, roles, or facility authorization is granted. Timeouts of cached credentials ensure user permissions and access are current. Organizations operating manufacturing systems should determine the time-period in which to prohibit the use of cached authenticators. Related Controls: None.
IA-7	Cryptographic Module Authentication	Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. This control should only be implemented in manufacturing systems that have the technical capability. Related Controls: AC-3, IA-5, SA-4, SC-12, SC-13
IA-8	Identification and Authentication (Non-Organizational Users)	Non-organizational users include system users other than organizational users explicitly covered by IA-2. Nonorganizational users are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. User identity must be confirmed prior to any system, roles, or facility authorization is granted. Particularly in manufacturing system environments, unauthorized system access by a non-organizational user could result in system failure, which could severely impede mission success and even result in physical damage or harm. Related Controls: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8
IA-8(1)	Identification and Authentication (Non-Organizational Users) |Acceptance	Acceptance of PIV credentials is only required for organizations that follow OMB Memorandum M-19-17 [OMB-M1917] (e.g., federal agencies and contractors).

Control ID	Control Name	Supplemental Guidance
	of PIV Credentials From Other Agencies	Related controls: PE-3
IR-4	Incident Handling	As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure that they have the capability to address events that are specific to embedded components and devices. Related controls: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.
IR-6	Incident Reporting	The organization should report incidents on a timely basis. CISA collaborates with international and private-sector computer emergency response teams (CERTs) to share control systems-related security incidents and mitigation measures. System owners should refer to CISA and NSA cybersecurity alerts and advisories addressing security incidents and mitigation measures. <https://www.cisa.gov/news-events/cybersecurity-advisories>; <https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/>. Related controls: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.
IR-6(1)	Incident Reporting | Automated Reporting	The automated mechanisms used to support the incident reporting process are not necessarily part of or connected to the OT. Related controls: IR-7
MA-4	Nonlocal Maintenance	Nonlocal maintenance and diagnostic activities are conducted by individuals communicating through a network, either an external network or an internal network. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Nonlocal maintenance in manufacturing system environments is commonplace. As such, organizations should implement two-factor authentication (2FA) measures on systems that receive nonlocal maintenance. 2FA is required in order to ensure that administrative accounts are being used with integrity. Utilizing 2FA may not be technically feasible for

Control ID	Control Name	Supplemental Guidance
		all manufacturing systems. Organizations operating manufacturing systems that lack this capability should establish alternative acceptable authentication measures. Related Controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.
PL-9	Central Management	Central management is the organization-wide management and implementation of flaw remediation processes. It includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation controls. Organizations that operate network-connected manufacturing systems should implement a centrally managed flow remediation process, where technically feasible. In cases where a manufacturing system is air gapped or does not have network connectivity, this control enhancement may not be applicable. The updated NIST SP 800-53, Rev 5 control language makes central planning an all-encompassing action for controls and processes not just the flaw remediation aspect found in Rev 4. Related Controls: PL-8, PM-9
RA-5	Vulnerability Monitoring and Scanning	The organization makes a risk-based determination of how to monitor or scan for vulnerabilities on their system. This may include active scanning, passive monitoring, or compensating controls, depending on the system being scanned. For example, vulnerability examination may be performed using passive monitoring and manual visual inspection to maintain an up-to-date inventory of assets. That inventory can be cross-referenced against a list of known vulnerabilities (e.g., NSA advisories, CISA advisories, NIST National Vulnerability Database). Production may need to be taken offline before active scans can be conducted. Scans are scheduled to occur during planned OT outages whenever possible. If vulnerability scanning tools are used on adjacent non-OT networks, extra care is taken to ensure that they do not mistakenly scan the OT network. Automated network scanning is not applicable to non-routable communications, such as serial networks. Compensating controls include providing a replicated or simulated system for conducting scans or host-based vulnerability applications.

Control ID	Control Name	Supplemental Guidance
		Related controls: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11
RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	Discoverable information includes technical or key personnel information that adversaries could obtain without compromising or breaching the system, for example, by collecting information the system is exposing or by conducting extensive web searches (e.g., technical forums, blogs, and vendor or contractor websites). Organizations should carefully consider the discoverable information in their manufacturing system environments and understand how an adversary could use that information to impact mission success. Additionally, active vulnerability scanning, which introduces network traffic, must be used with caution on manufacturing systems to ensure that manufacturing functions are not adversely impacted by the scanning process. When scanning is not permitted on active manufacturing systems, organizations should develop system-specific scanning procedures that consider the risk, requirements, and vulnerabilities of individual systems. Related Controls: AU-13, SC-26
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	Secure name/address resolution services should only be used after careful consideration and verification that they do not adversely impact the operational performance of the OT. Related controls: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Where feasible, organizations should ensure the systems that collectively provide name/address resolution services in a manufacturing system environment are fault-tolerant and implement internal and external role separation. If the systems of interest do not possess or require name/address resolution capabilities, this control is not applicable. Related Controls: SC-2, SC-20, SC-21, SC-24
SI-2	Flaw Remediation	Flaw remediation, or patching, is complicated since many OT employ operating systems and other software that are no longer maintained by the vendors. OT operators may also not have the resources or capability to test patches and are dependent on vendors to validate the operability of a patch. Sometimes, the organization has no choice but to

Control ID	Control Name	Supplemental Guidance
		accept additional risk if no vendor patch is available, if patching requires additional time to complete validation or testing, or if deployment requires an unacceptable operations shutdown. In these situations, compensating controls should be implemented (e.g., limiting the exposure of the vulnerable system, restricting vulnerable services, implementing virtual patching). 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 that the OT can identify exploitation of the flaw). Testing flaw remediation in an OT may exceed the organization's available resources. Related controls: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.
SI-4(14)	System Monitoring | Wireless Intrusion Detection	In manufacturing system environments with wireless connectivity, organizations should incorporate intrusion detection systems to identify rogue wireless device, detect attack attempts, and monitor wireless communications. This control is not applicable if wireless connectivity is not a factor in the manufacturing system environment. Related Controls: AC-18, IA-3
SI-4(15)	System Monitoring | Wireless to Wireline Communications	Wireless networks are inherently less secure than wired networks. As such, organizations should employ an intrusion detection system in their manufacturing system environment to monitor wireless communications traffic as the traffic passes from wireless to wireline (wired) networks. This control is not applicable if wireless connectivity is not a factor in the manufacturing system environment. Related Controls: AC-18
SI-8	Spam Protection	OT organizations implement spam protection by removing spam transport mechanisms, functions, and services (e.g., electronic mail, web browsing) from the OT. Related controls: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.
~~SI-8(2)~~	~~Spam Protection | Automatic Updates~~	This control has been removed from the overlay because spam transport mechanisms are disabled or removed from the OT, so automatic updates are not necessary.