Manufacturing Overlay

1. Overview

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 that complements and refines existing security control baselines and addresses security 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 security control Overlay that produces tailored cybersecurity guidance. Overall, this produced a manufacturing systems security control Overlay that provides a standardized approach to securely implementing tailored security controls for manufacturing systems within the DIB that complements the security control baselines established in the Department of Defense 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 Risk Management Framework (RMF) Knowledge Service (KS) for additional information regarding the development, background, tailoring, and applicability of the Manufacturing Overlay.

RMF KS: https://rmfks.osd.mil/rmf/Pages/default.aspx.

2. Scope and Applicability

This Manufacturing Overlay applies to systems, including control systems of any type, IoT 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

The objective of the FG is to produce an overlay tailored 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 information system owners and authorizing officials with preliminary security controls for DoD control systems supporting manufacturing processes. 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 have the ability to 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.

3. Controls

The Manufacturing Overlay Consists of 344 controls and control enhancements. The security control baseline leveraged information from NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security,* and was derived from the CNSSI 1253 Low-Low-Moderate security control baseline with a focus on manufacturing system environments. In the table below, an "**X**" indicates that supplemental guidance was developed for the control to address the unique security requirements of manufacturing systems.

Table 1: Manufacturing Overlay Control Baseline

Manufacturing Overlay		
Control ID	**Control Name**	**Supplemental Guidance Included**
AC-1	**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**	
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**	
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	**Policy and Procedures**	
AT-2	**Awareness Training**	

AT-2 (2)	**Awareness Training | Insider Threat**	
AT-3	**Role-based Training**	
AT-3 (2)	**Role-based Training | Physical Security Controls**	
AT-3 (4)	**Role-based Training | Suspicious Communications and Anomalous System Behavior**	
AT-4	**Training Records**	
AU-1	**Policy and Procedures**	
AU-2	**Event Logging**	**X**
AU-2 (3)	**Event Logging | Reviews and Updates**	
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**	
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-6 (10)	**Audit Record Review, Analysis, and Reporting | Audit Level Adjustment**	**X**
AU-8	**Time Stamps**	
AU-8 (1)	**Time Stamps | Synchronization with Authoritative Time Source**	
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 Capacity**	**X**
AU-12	**Audit Record Generation**	
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)	**Session Audit | System Start-up**	**X**
AU-14 (2)	**Session Audit | Capture and Record Content**	

AU-14 (3)	**Session Audit | Remote Viewing and Listening**	
CA-1	**Policy and Procedures**	
CA-2	**Control Assessments**	
CA-2 (1)	**Control Assessments | Independent Assessors**	
CA-3	**Information Exchange**	**X**
CA-3 (1)	**Information Exchange | Unclassified National Security System Connections**	
CA-3 (5)	**Information Exchange | Restrictions on External System Connections**	
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	**Policy and Procedures**	
CM-2	**Baseline Configuration**	
CM-2 (1)	**Baseline Configuration | Reviews and Updates**	
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 — Whitelisting**	
CM-8	**System Component Inventory**	
CM-8 (2)	**System Component Inventory | Automated Maintenance**	
CM-8 (3)	**System Component Inventory | Automated Unauthorized Component Detection**	
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	**Policy and Procedures**	
CP-2	**Contingency Plan**	
CP-2 (1)	**Contingency Plan | Coordinate with Related Plans**	
CP-2 (3)	**Contingency Plan | Resume Missions 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**	
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**	
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**	
CP-10 (2)	**System Recovery and Reconstitution | Transaction Recovery**	
IA-1	**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 (8)	**Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant**	
IA-2 (11)	**Identification and Authentication (organizational Users) | Remote Access — Separate Device**	
IA-2 (12)	**Identification and Authentication (organizational Users) | Acceptance of PIV Credentials**	
IA-3	**Device Identification and Authentication**	
IA-4	**Identifier Management**	
IA-5	**Authenticator Management**	
IA-5 (1)	**Authenticator Management | Password-based Authentication**	
IA-5 (4)	**Authenticator Management | Automated Support for Password Strength Determination**	
IA-5 (7)	**Authenticator Management | No Embedded Unencrypted Static Authenticators**	
IA-5 (8)	**Authenticator Management | Multiple System Accounts**	
IA-5 (11)	**Authenticator Management | Hardware Token-based Authentication**	
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**	
IA-8 (2)	**Identification and Authentication (non-organizational Users) | Acceptance of External Credentials**	
IA-8 (3)	**Identification and Authentication (non-organizational Users) | Use of FICAM-approved Products**	
IA-8 (4)	**Identification and Authentication (non-organizational Users) | Use of NIST-issued Profiles**	
IR-1	**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**	
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-5	**Incident Monitoring**	
IR-6	**Incident Reporting**	
IR-6 (1)	**Incident Reporting | Automated Reporting**	
IR-6 (2)	**Incident Reporting | Vulnerabilities Related to Incidents**	
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**	
IR-9	**Information Spillage Response**	
IR-9 (2)	**Information Spillage Response | Training**	
IR-10	**Incident Analysis**	
MA-1	**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	**Policy and Procedures**	
MP-2	**Media Access**	

MP-6	**Media Sanitization**	
MP-7	**Media Use**	
MP-7 (1)	**Media Use | Prohibit Use Without Owner**	
PE-1	**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 (3)	**Fire Protection | Automatic Fire Suppression**	
PE-14	**Environmental Controls**	
PE-15	**Water Damage Protection**	
PE-16	**Delivery and Removal**	
PE-17	**Alternate Work Site**	
PL-1	**Policy and Procedures**	
PL-2	**System Security and Privacy Plans**	
PL-2 (3)	**System Security and Privacy Plans | Plan and Coordinate with Other Organizational Entities**	
PL-4	**Rules of Behavior**	
PL-8	**Security and Privacy Architectures**	
PL-8 (1)	**Security and Privacy Architectures | Defense-in-depth**	
PM-1	**Information Security Program Plan**	
PM-2	**Information Security Program Leadership Role**	
PM-3	**Information Security and Privacy Resources**	
PM-4	**Plan of Action and Milestones**	
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	**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**	
RA-1	**Policy and Procedures**	
RA-2	**Security Categorization**	
RA-3	**Risk Assessment**	
RA-5	**Vulnerability Monitoring and Scanning**	
RA-5 (1)	**Vulnerability Monitoring and Scanning | Update Tool Capability**	
RA-5 (2)	**Vulnerability Monitoring and Scanning | Update System Vulnerabilities**	
RA-5 (4)	**Vulnerability Monitoring and Scanning | Discoverable Information**	**X**
RA-5 (5)	**Vulnerability Monitoring and Scanning | Privileged Access**	
SA-1	**Policy and Procedures**	
SA-2	**Allocation of Resources**	
SA-3	**System Development Life Cycle**	
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-12	**Supply Chain Protection**	
SA-15	**Development Process, Standards, and Tools**	
SA-15 (9)	**Development Process, Standards, and Tools | Use of Live Data**	
SA-19	**Component Authenticity**	
SC-1	**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 | Prevent 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**	
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-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)	**Mobile Code | Identify Unacceptable Code and Take Corrective Actions**	
SC-18 (2)	**Mobile Code | Acquisition, Development, and Use**	
SC-18 (3)	**Mobile Code | Prevent Downloading and Execution**	
SC-18 (4)	**Mobile Code | Prevent Automatic Execution**	
SC-19	**Voice Over Internet Protocol**	
SC-20	**Secure Name/address Resolution Service (authoritative Source)**	
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**	
SI-1	**Policy and Procedures**	
SI-2	**Flaw Remediation**	
SI-2 (1)	**Flaw Remediation | Central Management**	**X**
SI-2 (2)	**Flaw Remediation | Automated Flaw Remediation Status**	
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**	**X**

SI-3 (1)	**Malicious Code Protection | Central Management**	
SI-3 (2)	**Malicious Code Protection | Automatic Updates**	
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-7 (14)	**Software, Firmware, and Information Integrity | Binary or Machine Executable Code**	
SI-8	**Spam Protection**	
SI-8 (1)	**Spam Protection | Central Management**	
SI-8 (2)	**Spam Protection | Automatic Updates**	
SI-10	**Information Input Validation**	
SI-11	**Error Handling**	
SI-12	**Information Management and Retention**	

4. Supplemental Guidance

During the development of the Manufacturing Overlay, 29 controls were identified as requiring additional supplemental guidance. These controls include:

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

The specific control language developed to address the unique security requirements of manufacturing systems can be found in *Table 2: Manufacturing Overlay Supplemental Guidance.*

Table 2: Manufacturing Overlay Supplemental Guidance

Manufacturing System Supplemental Guidance		
Control ID	**Control Name**	**Supplemental Guidance**
AC-2 (4)	**Account Management | Automated Audit Actions**	The information 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 an information 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 an information system possessing these capabilities. As such, this control may not be applicable in particular scenarios. Related Controls: AU-2, AU-12
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: SC-23

AC-2 (12)	**Account Management | 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: CA-7
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
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: None
AC-22	**Publicly Accessible Content**	This control should be implemented in manufacturing systems that have the capability to push information to a publicly accessible information 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, AC-4, 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-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4
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 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-11, 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 (10)	**Audit Record Review, Analysis, and Reporting | Audit Level Adjustment**	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.

		This enhancement was removed and incorporated into AU-6 in NIST SP 800-53 Rev. 5 Related Controls: none
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 and/or transfer them to a more permanent medium. Related Controls: AU-4, AU-4 (1)
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, AU-12
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: AU-7
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 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, AU-4, AU-5, AU-9, AU-11
AU-14 (1)	**Session Audit | 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 (AO), Information System Security Manager (ISSM), Cyber Security Service Provider (CSSP)). 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-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4
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 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, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4
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 information 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 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-6, PE-3
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: 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. Non-organizational 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-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8
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 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, MP-6, PL-2, SC-7, SC-10, SC-17
RA-5 (4)	**Vulnerability Monitoring and Scanning | Discoverable Information**	Discoverable information includes 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. 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-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 (1)	**Flaw Remediation | 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. Related Controls: none
SI-3 (1)	**Malicious Code Protection | Central Management**	Central management addresses the organization-wide management and implementation of malicious code protection mechanisms. Organizations that operate network-connected manufacturing systems or have the technical capability for centrally managed malicious code protection mechanisms should do so. This is important to systems that are connected to networks. A central management of malicious code protection will provide indication of manufacturing systems suffering from malicious logic. This control enhancement may not be applicable to manufacturing system environments where centralized management is not a possibility. Related Controls: AU-2, SI-8

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