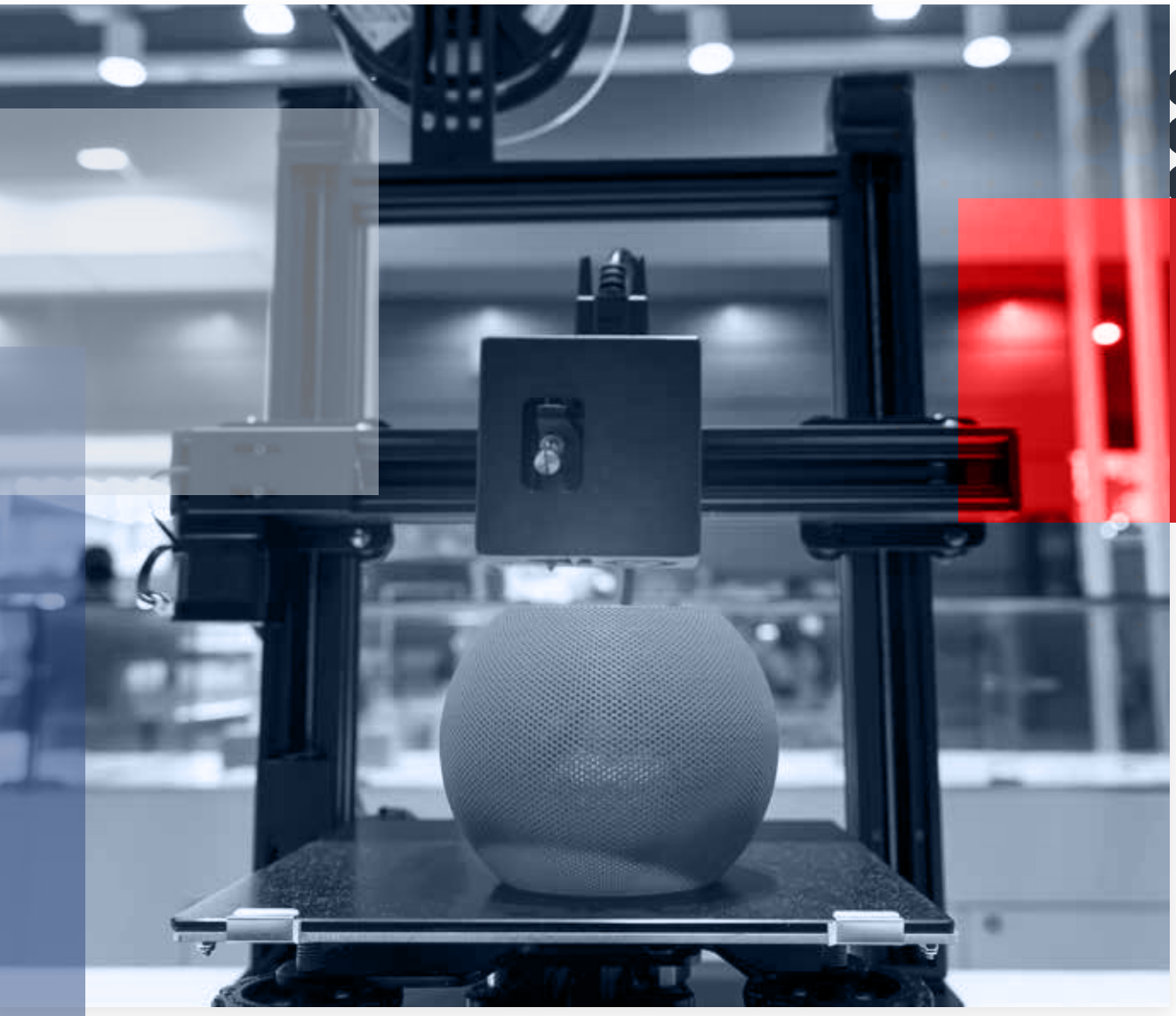
M D Cyber

PLAYBOOK SERIES



Ensuring Cybersecurity in Additive Manufacturing:

A Step-by-Step Guide for Additive Manufacturing or Manufacturing Environments

Playbook 2

MxD Cyber

PLAYBOOK SERIES

PLAYBOOK 2

Ensuring Cybersecurity in Additive Manufacturing

CONTACT:

MxD Cyber

cyber@mxdusa.org

MxD 1415 North Cherry Ave, Chicago, IL 60642

www.mxdusa.org

Table of Contents

1 Introduction **6**

1.1 Purpose & Intended Audience 7

1.2 Terminology 7

2 Understanding Cybersecurity Guidance Frameworks & Compliance **8**

2.1 Applying Cybersecurity to Additive Manufacturing 9

2.2 Introduction to the Risk Management Framework 10

2.3 Specific Cybersecurity Guidance for Industrial Control Systems: The ICS Overlay 12

3 Design Considerations for RMF Controls **13**

3.1 AC – Access Control 14

3.2 AT – Awareness and Training 16

3.3 AU – Audit and Accountability 16

3.4 CA – Assessment, Authorization, and Monitoring 17

3.5 CM – Configuration Management 18

3.6 CP – Contingency Planning 19

3.7 IA – Identification and Authentication 19

3.8 IR – Incident Response 21

3.9 MA – Maintenance 21

3.10 MP – Media Protection 22

3.11 PE – Physical and Environmental Protection 22

3.12 PL – Planning 22

3.13 PM – Program Management 22

3.14 PS – Personnel Security 23

3.15 PT – PII Processing and Transparency 23

3.16 RA – Risk Assessment 24

3.17 SA – System and Services Acquisition 24

3.18 SC – System and Communications Protection 25

3.19 SI – System and Information Integrity 27

3.20 SR – Supply Chain Risk Management 29

4 Approaches to Cybersecurity Compliance Documentation 30

Approaches to Cybersecurity Compliance Documentation 31

5 Vendor Cybersecurity Responsibilities During the DoD Acquisition Lifecycle 34

Vendor Cybersecurity Responsibilities During the DoD Acquisition Lifecycle 35

6 System Security Engineering Considerations 38

System Security Engineering Considerations 39

7 References 40

8 Appendix A: RMF Control Applicability Matrix 43

9 Appendix B: RMF Artifact Templates 45

Change Record

Revision	Date	Sections	Description
1.0	October 25, 2023	All	First official release

Distribution Statement

This project was completed under the Technology Investment Agreement No. W15QKN-19-3-0003, between Army Contracting Command – New Jersey MxD. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited

1 Introduction

1.1 Purpose & Intended Audience

This document addresses unique considerations for Department of Defense (DoD) Risk Management Framework (RMF) compliance, in the deployment of additive manufacturing (AM) devices. It is intended to supplement existing federal guidance, summarize relevant cybersecurity frameworks and processes, and clarify interpretation of certain system engineering requirements in the context of AM devices. At no point should the recommendations of this document be considered to supersede authoritative federal guidance but may be used in parallel with those requirements.

This document is primarily intended for AM device manufacturers and vendors who wish to incorporate the cybersecurity requirements of RMF into their product design and documentation to facilitate the acquisition process for current and potential DoD customers. AM cybersecurity is presented as a distinct subclass of industrial control system (ICS) security to meet the need for industry recommendations regarding this subject. Recommendations provided are for AM devices only and the software components used to control the devices. Authoritative guidance has been provided elsewhere for other components that may be used in the AM control network.

This document will elucidate the respective responsibilities of the vendor, the customer, and both parties in coordination of the process of ensuring secure operation of AM devices in deployment. Specifically, this document provides information for the following roles:

- System hardware and software engineers for design, integration, or implementation of AM systems.
- System administrators and service technicians for AM systems.
- Security consultants tasked with assessing compliance for AM systems.
- Contract writers tasked with incorporating provisions for cybersecurity requirements into proposals.
- System documentation authors.
- Senior management for strategic and business planning.

The division of responsibilities provided in this document reflects the most general case; thus, the scope is not exhaustive nor mandatory for every acquisition. This arises due the diversity of system types which the vendor may supply and the intended location for which the acquisition of such equipment is intended. Even in this regard, the fundamental distinction still holds that the vendor must supply the information pertaining to the design choices and intended operation of their product and the customer must supply their organizational procedures and the technical details of the installation IT under their control.

1.2 Terminology

The term “vendor” generalizes the role of the AM system developer, manufacturer, distributor, or integrator for the purposes of this document. It serves to describe the role of the party responsible for delivering the AM system to the DoD customer. More specific terminology is used when a greater specification of the role is needed.

The discussion of cybersecurity frameworks in this document applies to AM control systems, however, technical discussions have been limited to only the system components directly provided by the vendor, as guidance already exists for common components of control systems, such as workstations, switches, and controllers.

The components of an AM system are generalized to the terms “printer” and “application.” Printer is defined as the AM machine hardware, firmware, operating system, drivers, libraries, and specialized control software residing within the machine enclosure. The application is the software interface that relays information to and from the AM machine. This application may be installed on an onsite control workstation or be part of a remote/cloud deployment. The software that handles direct communication with the AM machine will often be integrated with a suite of programs that handle various aspects of AM manufacturing control and design. All manufacturer/vendor software that is installed on hardware components in the system scope are considered the application collectively.

This project was completed under the Technology Investment Agreement No. W15QKN-19-3-0003, between Army Contracting Command – New Jersey and MxD. Any opinions, findings and conclusions or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of any Department of Defense office. At no point should the recommendations of this document be considered to supersede authoritative federal guidance.

DISTRIBUTION STATEMENT A: Approved for public release: distribution unlimited.

2

Understanding Cybersecurity Guidance Frameworks & Compliance

2.1 Applying Cybersecurity to Additive Manufacturing

Additive manufacturing (AM) techniques continue to fulfill an ever more crucial role in modern supply chain automation. In itself, AM presents a facile alternative means to accomplish certain manufacturing processes that would otherwise require elaborate traditional machining or molding techniques. The capacity for automation by AM, however, enables potential benefits to supply chain efficiency beyond that of simplifying just one step of a manufacturing process. The trend of increased computer integration in manufacturing seeks to provide producers with a more robust, flexible, rapid, and lean manufacturing process. While automation principles can be applied effectively to any manufacturing technique, the unique nature of AM makes it one of the most readily amenable techniques to adapt to these principles.

It is the ability to integrate and automate business, logistical, and manufacturing processes over computer networks that yields the productive benefit of industrial automation. This increased integration and automation, however, subjects manufacturing control systems to an ever-greater number of cybersecurity threats.

The National Institute of Standards and Technology (NIST) defines cybersecurity as,

"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

Additive manufacturing systems face a variety of common and unique cyber threats that if improperly addressed can lead to adverse consequences to the organization that operates the equipment. Such threats include control system denial-of-service attacks or damage to the AM machines, unauthorized disclosure of potentially sensitive, private, or proprietary information, and unauthorized access to other organizational systems. A coherent mitigation approach for AM must take into account the unique requirements for these classes of control systems. This document is presented to AM industry stakeholders to provide information regarding the cybersecurity considerations during a DoD acquisition.

2.2 Introduction to the Risk Management Framework

The Risk Management Framework (RMF) was developed by the National Institute of Standards and Technology (NIST) as a standardized, risk-based approach to secure federal information systems and communication technology.

It is a lifecycle process used to secure, assess, authorize, and maintain accreditation for DoD systems. RMF incorporates U.S. federal government policy and standards to help secure information systems and DoD data. It integrates information security and risk management activities into system development, procurement, deployment, maintenance, and decommissioning.

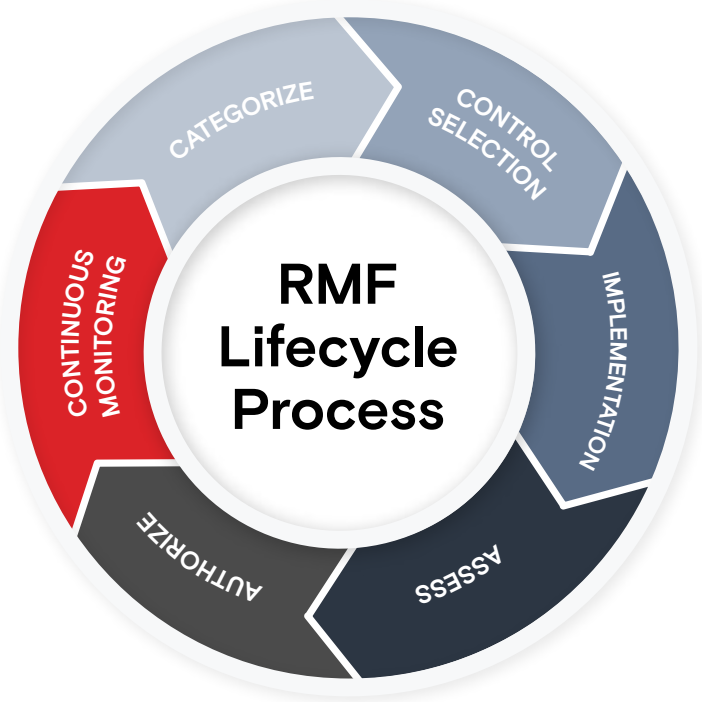
NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy*, was developed to help organizations manage security and privacy risk, and to satisfy the requirements in the Federal Information Security Modernization Act of 2014 (FISMA), the Privacy Act of 1974, Office of Management and Budget (OMB) policies, and Federal Information Processing Standards (FIPS), among other laws, regulations, and policies. This serves as the foundational document for the RMF, which provides a standard framework for managing risk to federal organizations in operating information systems. This framework is applied to all information systems formally operated by the federal government.

Although a detailed description of the RMF process is beyond the scope of this document, it is important for AM vendors looking to conduct business with federal entities or their contractors to understand the significant aspects of the government approach to cybersecurity. It is an unfortunate fact that too often misconceptions of the RMF lead to loss of time and money, unnecessary work, and potential risk. A structured approach to cybersecurity by the vendor from product design onward can facilitate the process for the customer, produce a safer and more robust product, and potentially give the vendor a competitive edge in the market.

Formal Risk Management

Every information system is subject to an array of *threats* - events which, intentionally or unintentionally, can adversely affect system confidentiality, integrity, or availability (C-I-A). There is an associated *risk* for each threat to the system which is a function of the adverse *impact* a threat occurrence would have on the organization and the *likelihood* of such an occurrence. As the name implies, RMF is concerned with applying measures to reduce risk to acceptable levels. Finite resources and unknown factors make it impossible to completely eliminate risk, so threats with high impact and high likelihood are generally prioritized. This is a salient point. Leaving the wrong door unlocked in a building can have the same devastating effect as an elaborate zero-day code-injection exploit researched and developed for months by a large hostile organization. The difference is that the former event can have a much higher likelihood if the organization does not take the proper precautions. Likewise, when we speak of impact, we mean impact to the organization and its mission as a whole, not to the system itself *per se*. A visitor information kiosk in a public lobby is simply less important than, say, an organization's finance database.

The RMF is intended to provide an objective measure for organizations to make judgments of this kind. NIST defines a number of general actions to handle risk, the most important of which is *risk mitigation* which is defined as a measure taken to reduce the either the impact or likelihood of a given threat, thereby reducing the risk. Risk mitigation in RMF is accomplished by the implementation of *security controls* – organizational or technical processes that are placed under formal control and enforced by organizational policy. Security controls for RMF have been compiled and described by NIST in NIST SP 800-53. Organizations apply RMF security controls based on the unique circumstances of information system operation and capabilities. Some controls are implemented through a policy applied to the organization as a whole. Other controls are system-specific technical measures. Technical controls are applied to the system as a whole, so different components will have different requirements based on the control. RMF does not make a formal distinction between strictly policy and strictly technical controls. There is often an element of both necessary to meet the intent of the control.

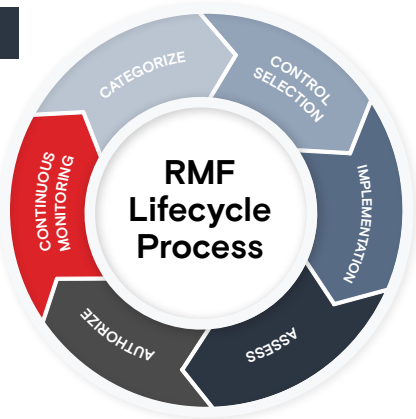


RMF Lifecycle Process

RMF activities are conducted throughout the entirety of the system lifecycle; from provisioning and acquisition all the way to final decommissioning. The tasks of RMF are grouped into six major steps which compose the RMF cycle.

1 CATEGORIZE

When a new system is registered, the first step is to determine the C-I-A impact levels for the system and the data contained therein. It is at this phase that a system description document should be drafted and key RMF roles assigned.



2 CONTROL SELECTION

When the C-I-A categorization for a system is made, the organization makes a selection of security controls commensurate with the impact levels of the system. NIST's suggested control baselines are given in NIST SP 800-53B. The DoD and several other federal agencies use CNSSI 1253 as authoritative guidance to establish a control baseline. The control selections in CNSSI 1253 are derived from NIST SP 800-53B with a few modifications and include additional control requirements for designated national security systems (NSS) as defined by CNSSI 4009 (ultimately required under the provisions of 44 U.S.C. 3542). It is at this stage that control overlays, such as the ICS Overlay, are applied to the control baseline to meet the specific requirements for the system type and usage. Organizations have the liberty to further tailor the control baseline as appropriate for their system. This may include the addition of an organization-specific overlay or the removal of non-applicable controls (a control may be non-applicable, for instance, if the system does not support the functionality that the control addresses so there is no risk to mitigate). With a control selection made, the organization may produce a preliminary security and privacy plan for the system. The control selection and security plan must be approved by the authorizing official before proceeding to the next step.

3 IMPLEMENTATION

During this stage, system design and configuration settings are applied, and organizational policies are enacted in order to address the security controls identified in the security plan. The relevant system artifacts are drafted at this time and incorporated into the RMF package. Progress is tracked in the RMF Implementation Plan. The majority of the system owner's RMF efforts will occur during this stage. Security measures identified in the security plan that are not fully implemented in the time allocated for this stage must be listed in the system's Plan of Action and Milestones (POAM) document, that identifies each control correlation identifier (CCI) that remains to be met, a timeframe for mitigation, and a brief narrative of the intended mitigation course of action and organizational responsibilities.

4 ASSESS

A completed RMF package is required to be submitted for a third-party assessment by an organization's security controls assessor (SCA). NIST SP 800-53A is used as the formal framework for making the assessment. In this publication, a list of "Assessment Procedures" (APs) are given for each control which are verifiable statements regarding the implementation of various aspects of each control. For instance, if a control has both a policy and technical requirement there will be one or more APs covering the existence of policy and covering the technical settings for the system. This permits a greater degree of granularity in the assessment. All APs for a control must be met for a control to be considered implemented. In practice, one often speaks of meeting CCIs during an assessment. These are a set of verifiable statements published by Defense Information Systems Agency (DISA) which form a roughly one-to-one correspondence with the NIST assessment procedures, but contain modifications to the language to better suit the purposes of the DoD. These may be considered to serve a roughly interchangeable role for most purposes of RMF. NIST SP 800-53A also provides the assessor a wide variety of methods for verifying the application of each security control, ranging from examining system documentation and artifacts, to interviewing responsible organizational personnel, to performing diagnostic tests of the system itself. Assessments may be official or unofficial. Since an official, exhaustive assessment of a system constitutes a considerable undertaking, system owners almost always conduct more limited, unofficial assessments either by themselves or by a third-party assessor to ensure correct application of RMF requirements prior to investing the resources in an official assessment. The results of an assessment, official or otherwise, are documented in a Test Results document that records the then current status of each AP/CCI applicable to the system with a brief narrative of the method used to determine the status. The system owner is given an opportunity to review the official assessment findings and address any SCA recommendations prior to proceeding to the next stage.

5 AUTHORIZE

The authorizing official (AO) is an individual with a command position in the organization who is tasked, following a review of the RMF package submitted by the system owner and the findings of the SCA, with making the determination whether the implemented security measures mitigate the risk to the organization in operating the system to a tolerable level. This culminates in the granting or denial of authority to operate (ATO) the system within the parameters set by the security plan. The DoD expands upon the RMF process formulated by NIST by defining several recognized kinds of authorization to better suit its organizational needs. It is a distinct feature of RMF that the AO must make the authorization to accept or deny the risk incurred to the organization in granting ATO as an individual, and must accept full responsibility for the decision. This was designed to enforce a high degree of accountability for the AO which is passed on to all other parties by extension and thus ensure the entire process is taken seriously. The general ATO is granted for three years.

6 CONTINUOUS MONITORING

The system security plan will specify the periodic actions the system owner must take to ensure continuing application of identified security controls during the system lifecycle following ATO.

Hierarchy of RMF

To enforce a unified approach to cybersecurity policy in an organization, RMF incorporates an inheritance mechanism for controls. Policy-based controls may be defined at three levels within the organization as defined by NIST SP 800-37: Tier 1 – Organization-wide controls, Tier 2 – Mission/Business Process controls, and Tier 3 – Information system-specific controls. Compliance with controls defined at Tier 1 and Tier 2 can be assured by adopting that control policy for the system. These controls are then said to be inherited. Inheritance may also be defined at the CCI / AP level to provide a greater degree of granularity. Controls that are partially inherited are said to be hybrid controls and will require the system owner to implement the uninherited CCIs. Hybrid controls are useful for defining an organization-wide policy governing a certain system attribute for which the actual configuration to implement the policy will vary with the system type.

For the DoD, Tier 1 inheritance is DoD-wide, Tier 2 inheritance originates from DoD component commands.

DoD Distinctive RMF Concepts

DoDI 8500.01 contains the DoD-wide instruction for cybersecurity. The DoD implementation of RMF is given in DoDI 8510.01. Here the RMF definitions, roles, responsibilities, and formal process for the DoD are specified. The DoD adopts the RMF from NIST with a number of extensions to better suit its purposes. These are mentioned in passing here. The first is the categorization of DoD information technology into information systems, platform IT (PIT and PIT systems), IT services, and IT products. This guides the determination of what systems of components must undergo full authorization, and which are assess only. The second is the mechanism of reciprocity, where rules are defined for one DoD entity to leverage an existing ATO belonging to another DoD entity for the same kind of system. A stronger form of reciprocity is the type authorization, which allows a single security authorization package to be developed for an archetype "common" version of a system, and the issuance of a single authorization decision (ATO) that is applicable to multiple deployed instances of the system.

2.3 Specific Cybersecurity Guidance for Industrial Control Systems: The ICS Overlay

Industrial Control Systems/Occupational Technology Systems (ICS/OT) differ in functionality and composition from traditional enterprise IT networks. In general risk management terms, the priority of ICS is first availability, then integrity, and lastly confidentiality. It is the process control functionality of the system and not the system data that is the primary concern for protection, although for AM control systems this convention is lessened somewhat.

NIST has provided distinct guidance for ICS/OT cybersecurity in NIST SP 800-82. In addition to general ICS guidance and security control interpretations for these systems, this publication also defines the ICS control overlay. Overlays are sets of controls either added or removed from a control baseline to further tailor it for a specific situation. AM control systems will normally have the ICS overlay applied to the selected control baseline.

ICS architecture is often analyzed against the *Purdue Enterprise Reference Architecture* (PERA). Contemporary variations of the model categorize ICS components into the following hierarchy:

- **Enterprise Zone** (The organization's traditional IT network)
    - Level 5 – Organization-wide enterprise IT
    - Level 4 – Site enterprise IT
- **ICS Demilitarized Zone** (ICS DMZ, sometimes also called "Level 3.5")
- **Control Zone** (The ICS network proper)
    - Level 3 – Site manufacturing and operations control
    - Level 2 – Area supervisory control
    - Level 1 – Basic process control
    - Level 0 – Physical process / equipment under control

The Purdue Model is useful to bear in mind in the following discussions. In an AM control system, the printer would occupy Level 1 of the model, directly controlling the physical process of printing. The application may reside at Levels 2 and 3 for a standalone system and for a system integrated into the enterprise IT architecture may have components in Levels 4, 5, and the ICS DMZ as well. The ICS DMZ serves the purpose of isolating the components in the ICS from external networks. It is assumed to be present in the following discussions of AM control systems that are intended to be integrated into the enterprise network.

NIST SP 1800-32B provides cybersecurity guidance for more nontraditional distributed industrial system architectures, sometimes called industrial internet of things (IIoT). These recommendations may be of interest to developers of emerging AM applications.

3

Design Considerations for RMF Controls

Please see Appendix A for control listing and applicability information.

3.1 AC – Access Control

Access Control family controls place personnel authorizations, rules of conduct, and mechanisms for accessing the information system under formal organizational control.

ACCOUNT MANAGEMENT

Applicability: Application, (Control System)
Impact: Low
Security Controls: AC-2, AC-2(3), AC-2(4), AC-2(5)
References: NIST SP 800-53, NIST SP 800-82

In a typical deployment, accounts for authorized system users will be handled by a front-end workstation or domain controller in the ICS network. This is the general preferred system architecture for account management in ICS. This way, compliance with access control requirements may be met through implementation of existing guidance for these controls, by application of relevant Security Technical Implementation Guide/Security Requirements Guide (STIG/SRG) guidance on the workstation OS and/or domain controller. There is an exception if the printer application permits remote network user access through a client-server model, in which case there must be a mechanism to restrict access to only authorized users. This is only relevant if the user interface component of the application and the printer control software component are separated over a remote network, for example, if a user must log into the printer control server through a client application or a web portal. For purposes of this discussion remote indicates remote with respect to the ICS system proper, i.e. Levels 4 and above in the Purdue Model. Otherwise, access control to the application is enforced through access control to the ICS system itself.

A distinction is made between user accounts in the organizational sense and user accounts in the operating system sense. The printer will generally have accounts in the operating system sense, almost certainly a root or administrator account and perhaps a separate system account to run the printer software. These will generally not be changed nor provided to organizational personnel for system access and thus fail to meet the organizational sense of the user account. Therefore, interface with these is conducted during maintenance and is controlled though the maintenance control family.

ACCESS AND INFORMATION FLOW ENFORCEMENT

Applicability: Printer, Application, (Control System)
Impact: Low
Security Controls: AC-3, AC-4
References: NIST SP 800-53, NIST SP 800-82

Each system component serves a different role for enforcement of access control and information flow in the system based upon the purpose and intended use of the component. These controls are largely met in the overall design of the control system, however, there may be distinct configuration requirements in key components in the form of STIG/SRG rules for these controls. For instance, a front-end workstation or front-end server will serve a key role in system-wide access control and system switches will serve a key role in information flow enforcement. Interpretation of these controls for the printer and application form what may be thought of as a negative requirement, in that the vendor should ensure the components should not provide unnecessary or undesired functionality. Physical access to the printer should not permit logical access to the greater control system. Please note that a minimal interface on the printer to control basic functions, such as an LCD screen with a keycode, is not in violation of the intent of these or other access control family controls, as this does not provide general access to the greater control system. Depending on the architecture of the application, it may or may not provide user access control to system data, functionality, or administration. Generally, this would only be the case if the application includes a server for a remote access portal, in which case it should handle access control in accordance with the Application Security and Development (ASD) SRG and other authoritative RMF guidance. Information flow control is considered at the conceptual level, abstracting the details of technical implementation to achieve the control. Organizations will have varying requirements for what classes of information, based on its security attributes, may reside or be transmitted within the system or between systems. The vendor should consider when implementing technical measures for securing communication between the printer and application how these measures may serve to control information flow.

LOGON AND SESSION MANAGEMENT

Applicability: Application, (Control System)
Impact: Low
Security Controls: AC-7, AC-8, AC-11, AC-11(1), AC-12
References: NIST SP 800-53, NIST SP 800-82

System user interfaces are subject to several distinct requirements in RMF. Any user interface must allow only a limited number of logon attempts in a defined period of time. The DoD has defined this requirement as three invalid logon attempts in a 15-minute period before the interface must be locked. The default DoD requirement is that the interface remain locked until released by a system administrator. In control systems where this would prove impractical, a time limit to automatically unlock the interface may be negotiated with the system owner. There should be a five second delay between logon attempts.

User interfaces must display the use notification banner DTM 08-060, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement." This is usually displayed on the interface screen, although this banner may be physically displayed on system components without a graphic user interface (GUI).

The DoD requires that a user interface must initiate a session lock after 15 minutes of inactivity and permit the user to manually initiate a session lock at any time. This lock need not halt or terminate a running process initiated by the user, only that the user must reenter credentials to continue interaction with the interface. When session lock is in effect, the contents of the interface must be obscured by a pattern-hiding display until credentials are reentered.

The user must have the ability to manually initiate a session termination, which halts all user-initiated running processes, at any time. A set of criteria must be defined for the system to automatically initiate a session termination and must be determined at a system-specific level to accommodate system availability requirements.

These requirements are applicable to all user interfaces regardless of how they are implemented. In the printer control system, these will likely be provided by a workstation operating system or the network. The vendor must take consideration whether the printer or application have a system user interface.

REMOTE ACCESS CONTROL

Applicability: Application, (Control System)
Impact: Low
Security Controls: AC-17, AC-17(1), AC-17(2)
References: NIST SP 800-53, NIST SP 800-82

A properly designed ICS system is deployed in an isolated, dedicated network which cannot directly communicate with external networks. As such, neither the printer nor any other component of the ICS network proper should have the capability of directly mediating remote access to the system. Print requests from remote locations, if allowed, should be handled by the organization's enterprise IT network, either the site network for the installation hosting the printer or in a cloud deployment. In this setup, the portion of the application that receives, verifies, and authenticates print requests from users is a separate software component from the portion of the application that controls the printer. The remote application server should handle user identification and authorization from remote clients in conformity with the requirements of the ASD SRG. Ideally, this portion of the application would provide input verification of the print files and permit the organization to specify the priority of print requests. The remote application server is subject to the security requirements of the organization's enterprise IT system in accordance with established guidance when deployed as part of it, which may differ from those of the ICS system proper. In all circumstances, any remote access to the system should be limited to requests for print functionality with all other functions, such as system configuration, being handled by onsite personnel. Information about the status of print jobs or information supporting logistical decisions can originate from the application.

Verified print requests should be routed through the ICS DMZ to be handled by the printer controller portion of the application such that a separation of the IT and ICS networks is maintained. Throughout the process of submitting remote print requests, primarily confidentiality and secondly integrity of the information is the highest priority. This is supported by both the vendor in following secure software development and communication security techniques and the organization in network architecture and access policies.

Note that during maintenance, the technician may establish a remote interface or terminal with the printer operating system to effect repairs or changes. This form of access is not considered under the heading of remote access considered by NIST which involves communication over networks external to the organization. Procedures for this interaction are regulated by the Maintenance family of controls.

WIRELESS ACCESS CONTROL

Applicability: Printer
Impact: Low
Security Controls: AC-18, AC-18(1), AC-18(3)
References: NIST SP 800-53, NIST SP 800-82

To best address differing compliance requirements for customers, the vendor should design the printer to provide a means for the customer to logically or physically disable any wireless communication technologies used by the printer. The vendor may elect to make the inclusion of a wireless interface optional at the time of purchase. If the interface hardware permits, allowing the user to adjust wireless signal power levels can help the customer restrict the physical range of wireless communications within a facility. Wireless communication protocols commonly encountered in ICS applications vary greatly in regards to authentication and encryption strength, and consequently in their degree of vulnerability to various wireless-based attacks. Since data transmitted to the printer may be considered sensitive by the organization, the vendor should use only wireless protocols with strong authentication and encryption that would be suitable in a more traditional IT environment of similar security categorization.

3.2 AT – Awareness and Training

The Awareness and Training control family ensures that system users and administrators receive appropriate basic and role-specific information security training, and that the organization maintains personnel training records.

These controls are handled at the organizational level and are inherited from DoD-level or component-level policy. The vendor is not directly responsible for implementation of any of the controls in this family but may indirectly facilitate the process by providing detailed system documentation.

Depending on the details of the system acquisition, the vendor may be required by the customer to provide lecture-based or hands-on training for system operation and administration. This requirement will be communicated through specific contract provisions. If vendor-provided training is used in fulfillment of RMF provisions, this will be documented by the gaining organization.

3.3 AU – Audit and Accountability

Audit and Accountability controls deal with the generation and management of event logs to establish a record of system operation to help detect anomalies and support incident investigations.

An important feature of auditing is establishing non-repudiation, enforcing accountability for system users regarding their actions on the information system.

EVENT TYPES, AUDIT RECORD CONTENT, AND AUDIT RECORD GENERATION

Applicability: Printer
Impact: Low
Security Controls: AU-2, AU-3, AU-3(1), AU-12
References: NIST SP 800-53, NIST SP 800-82

Logging is required for events that are significant and critical to the security of a system. Event logging also aids in the fulfillment of particular monitoring and audit record needs.

The DoD has defined the information system auditable events as:

- Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g. classification levels).
- Successful and unsuccessful logon attempts, Privileged activities or other system level access,
- Starting and ending time for user access to the system,
- Concurrent logons from different workstations,
- Successful and unsuccessful accesses to objects,
- All program initiations,
- All direct access to the information system.
- All account creations, modifications, disabling, and terminations.
- All kernel module load, unload, and restart.

The DoD requires audit records include the following information:

- Event type, description, and identification number
- Date and time which the event occurred
- The information system component or subsystem within which the event occurred
- The user identifier, process identifier, file, executable, module, network connection, network source or destination address, socket, or any other system element which is the source of the event
- The success or failure of the event in addition to all relevant event-specific outcomes
- The identity of the individual or subject associated with the event and the access control or flow control rules invoked

Additional audit record information for moderate impact systems must include at a minimum: full-text recording of privileged commands or the individual identities of group account users. The additional information must provide sufficient detail to reconstruct events to determine cause of compromise and magnitude of damage, malfunction, or security violation.

System components must comply with STIG/SRG guidance where applicable. While devices running a full OS should be able to comply with all DoD audit record requirements, the limited capabilities of the printer may preclude some of the event types. In this case, it is important to indicate to the customer what the printer can audit.

AUDIT LOG STORAGE CAPACITY AND AUDIT FAILURE BEHAVIOR

- **Applicability:** Printer, Application, (Control System)
- **Impact:** Low
- **Security Controls:** AU-4, AU-5
- **References:** NIST SP 800-53, NIST SP 800-82

The vendor should allocate sufficient audit log storage capacity to avoid audit data loss or audit logging capabilities. Audit log storage for ICS controllers is often expressed in a minimum number of days of guaranteed audit log persistence. Sixty days is common. When the assigned storage is at 75% of its maximum audit logging capacity, an error notification should be provided, if possible. This should also be provided for more general failures of the audit system.

In the case of audit storage failure, the printer should overwrite the oldest audit logs. The audit log ideally should be retrievable either by the application interface or by directly connecting to the printer.

AUDIT TIME STAMPS

- **Applicability:** Printer
- **Impact:** Low
- **Security Controls:** AU-8
- **References:** NIST SP 800-53, NIST SP 800-82

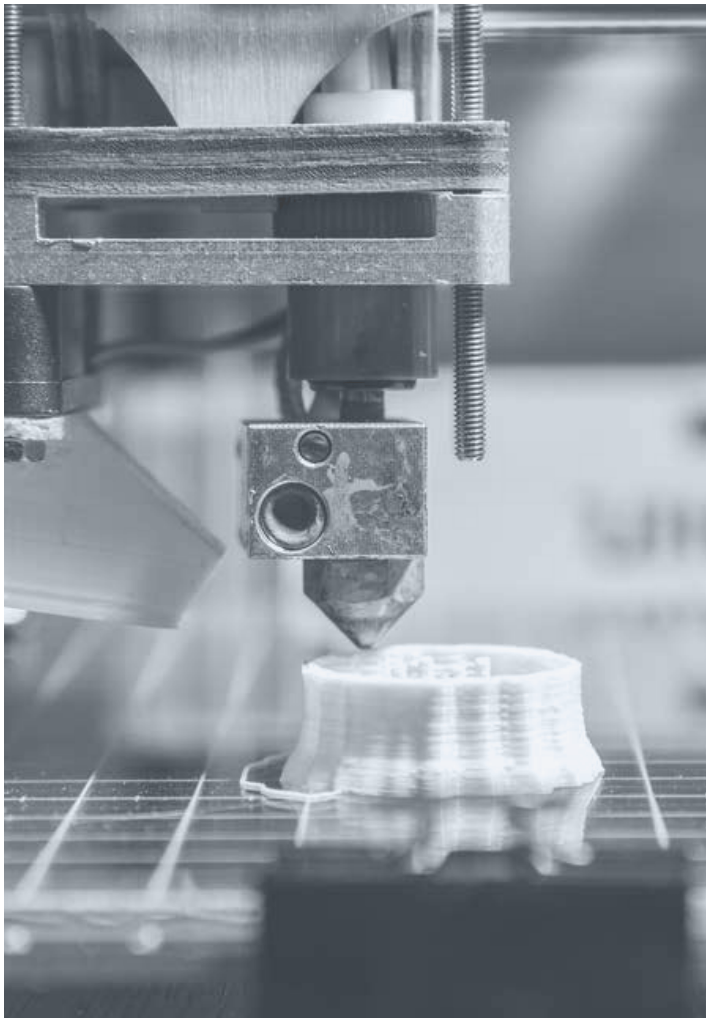
Audit records must be timestamped in Coordinated Universal Time (UTC), or local time offset from UTC. The granularity of time measurement must be at most one second.

PROTECTION OF AUDIT INFORMATION

- **Applicability:** Printer
- **Impact:** Low
- **Security Controls:** AU-9
- **References:** NIST SP 800-53, NIST SP 800-82

It is important to protect auditing information and tools safe against unauthorized access, modification, or destruction. Audit information is protected using both media protection and physical and environmental controls (i.e., limited physical access, media sanitization, and secure storage) which are primally the responsibility of the organization to implement.

In the printer, the means of audit record protection will reflect the general data-at-rest protections for the device.



3.4 CA – Assessment, Authorization, and Monitoring

The Assessment, Authorization, and Monitoring control family ensure specific plans and responsibilities for these steps of the RMF process are formally defined and controlled in the system security plan.

These controls are handled at the organizational level and are largely inherited from DoD and Component level policy.

3.5 CM – Configuration Management

Configuration Management controls ensure system settings and composition are maintained under formal organizational control.

CONFIGURATION SETTINGS AND BASELINE

- **Applicability:** Printer, Application
- **Impact:** Low
- **Security Controls:** CM-2, CM-6
- **References:** NIST SP 800-53

Configuration settings for the printer should be provided by the vendor but it is imperative that the organization have the systems security posture in place in accordance with STIG/SRG guidance. These configurations settings will provide the baseline parameters.

The baseline configuration provided by the vendor should be used as reference point for the organization to compare to current configurations. This would help the organization identify any anomalies or deviation configurations based off the baseline. The vendor should consider adding a backup default toggle that would allow the organization to restore the baseline configurations. The baseline should be configured in accordance with STIG/SRG guidance.

LEAST FUNCTIONALITY

- **Applicability:** Printer, Application
- **Impact:** Low
- **Security Controls:** CM-7
- **References:** NIST SP 800-53

The organization should consider having only the minimal functionality necessary to fulfill the mission. This could be accomplished by restricting user account functions to only what is necessary to perform, limiting the printer's connectivity to the network, and disabling the unnecessary printer functions.

PROGRAM EXECUTION RESTRICTIONS

- **Applicability:** Printer
- **Impact:** Moderate
- **Security Controls:** CM-7(2)
- **References:** NIST SP 800-53

Restricting application execution is a process used to prevent execution of unauthorized applications to adhere to the principle of least privilege. The organization should configure the system in accordance with STIG/SRG guidance and then follow the STIG/SRG guidelines to whitelist the printer application.

3.6 CP – Contingency Planning

The Contingency Planning control family addresses how the organization can maintain essential mission functions following a disruption to the system.

SYSTEM BACKUP, RECOVERY, AND RECONSTITUTION

- **Applicability:** Printer
- **Impact:** Low
- **Security Controls:** CP-9, CP-10
- **References:** NIST SP 800-53, NIST SP 800-82

Following an incident, a customer may need to reset or reinstall a recovery image and firmware for the printer. Depending on contractual details the vendor may be required to dispatch a service technician to perform a restoration of the printer or provide a recovery image for customer personnel to deploy. The details of this process should be stated explicitly in the service level agreement or in the system documentation.

As availability is the overriding concern of industrial control systems, the vendor should aim to refine the recovery procedure for the printer to minimize downtime. The vendor should test and benchmark the time for the recovery procedure internally, as a service level agreement may define a mean time to repair for which the vendor will be expected to uphold.

Ideally, the printer should be fully functional following reinstallation of a recovery image with a minimum of further configuration. Depending on how many user settings the printer configuration allows, it may be useful for the vendor to provide a mechanism for the user to backup printer configuration settings to an external file so that these may be applied automatically during the recovery process.

3.7 IA – Identification and Authentication

USER AUTHENTICATION

- **Applicability:** Printer, Application, (Control System)
- **Impact:** Low
- **Security Controls:** IA-2, IA-2(1), IA-2(2), IA-2(8), IA-2(12)
- **References:** NIST SP 800-53, NIST SP 800-82

The system must uniquely identify and authenticate system users. In an AM system deployment, users will primarily logon a control system workstation for a local system or potentially through a remote portal provided by the application. The primary user interfaces must fully comply with all identification and authentication controls selected for the system and apply and relevant STIG/SRG guidance. Password authentication is required for all system interfaces. DoD further requires multifactor authentication for network access to privileged and non-privileged accounts. For enterprise systems, this is typically accomplished using DoD common access card (CAC) credentials, which serve as the Personal Identity Verification (PIV) credentials for RMF purposes. A remote access interface will need to incorporate this requirement, although care should be taken during design of the application to ensure that verification requests of CAC credentials are handled outside the ICS DMZ. For isolated systems, implementation of multifactor authentication has always presented more of a challenge. The most common means of implementation is with token-based multifactor authentication, such as RSA tokens. This fulfills the multifactor requirement without issue.

Some devices in the AM control system, such as the printer, may have maintenance accounts. A minimum of a password requirement should be applied to these. Where compensating controls, usually physical security, are in place the exclusion of the multifactor requirement may be reasonably justified.

DEVICE AUTHENTICATION

Applicability: Printer, Application
Impact: Moderate
Security Controls: IA-3
References: NIST SP 800-53, NIST SP 800-82

The DoD has defined the devices subject to device authentication requirements as: "DoD has defined the value as all mobile devices and network connected endpoint devices (including but not limited to: workstations, printers, servers (outside a datacenter), VoIP Phones, VTC CODECs)." A 3D printer meets the definition of a network connected endpoint and is expected to have the capability of supporting device authentication. Device authentication may be implemented at different levels of the Open Systems Interconnection (OSI) network communication model. IEEE 802.1x is a common example of a device authentication protocol. Transport layer security (TLS)-level mechanisms also fulfill the requirement.

While this control contemplates authentication for a device to connect to the local network, the use of TLS certificates may be used to restrict communication between the application and printer to ensure only registered devices may be controlled, providing a further level of authentication.

Applicable STIG/SRG guidance for this control should be applied to relevant devices.

IDENTIFIER MANAGEMENT

Applicability: Printer, Application
Impact: Low
Security Controls: IA-4
References: NIST SP 800-53, NIST SP 800-82

Unique identifiers for all AM system users and devices are required. Typical examples include usernames for users and MAC and IP addresses for devices. The customer must establish a formal procedure for managing user and device identifiers, so it is critical for the vendor to make clear how these identifiers may be used and configured in the system.

AUTHENTICATOR MANAGEMENT

Applicability: Printer, Application, (Control System)
Impact: Low
Security Controls: IA-5, IA-5(1), IA-5(2)
References: NIST SP 800-53, NIST SP 800-82

It is required that organizations take measures to protect and restrict system authenticators. These include passwords as well as factors used in multifactor authentication such as tokens or biometric data. The customer will generate their own authenticators, so the vendor's primary task is to communicate how these are managed in the system. It is also important for the vendor to notify the customer of all default or temporary authenticators used in the system so that these may be changed immediately upon handover.

The system itself should be configured to reject any authenticators entered that do not meet customer requirements for security. Any applicable STIG/SRG guidance must be applied to relevant components.

The DoD requirements for all passwords are as follows:

- A minimum of 15 characters in length.
- A complexity requirement of at least one of each character type: Upper-case, Lower-case, Numeric, Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _ + = - ‘ [ ] / ? > <).
- At least fifty percent (50%) of the total number of characters must be changed when creating a new password. The number of characters refers to the number changes required with respect to the total number of positions in current password. In other words, characters may be the same within the passwords; however, the positions of the like characters must be different.
- The system must store and transmit only salted, one-way encrypted representations of passwords.
- The system must be configured to enforce a minimum password lifetime of twenty-four (24) hours and a maximum password lifetime of sixty (60) days.

The DoD requirements for public key infrastructure (PKI)-based authentication are as follows:

- The information system performing hardware token-based authentication must be configured to validate DoD-approved PKI credentials in accordance with RFC 5280.
- The information system must be configured to perform a revocation check as part of the certificate validation process. Revocation checking may be performed using certificate revocation lists (CRLs) published by the issuing PKI or Online Certificate Status Protocol (OCSP) services.
- Information systems must not have access to users' private keys. The cryptographic container in which the private keys are stored (e.g. smart card or software module) implements access controls and protections to ensure that only the authorized user can activate the private key. DoD users agree to protect their PKI credentials in accordance with the DD-2842 agreement that is executed for each credential. They are reminded of these responsibilities in annual information assurance (IA) training.
- The private key identifying the information system must be stored in a cryptographic container that is FIPS 140-2 validated. Only authorized information system operators should have access to activation data (e.g. password or PIN) for the private key.
- The information system performing PKI-based authentication must be configured to map the authenticated PKI credential to a corresponding network or information system account or role in accordance with DoDI 8520.03.
- The information system must be configured to locally cache revocation data to support path discovery and validation in case of inability to access revocation information via the network. The information system may meet this requirement by locally CRLs, OCSP responses, or a combination thereof.

- Cached revocation data must include revocation information from all PKIs serving known or anticipated users of the information system. Cached data must be refreshed with a frequency shorter than the life of the data (e.g. if a CRL is valid for 7 days, a new CRL must be retrieved and cached more frequently than every 7 days) to ensure that cached data is valid and not expired.

AUTHENTICATOR FEEDBACK

Applicability: Application, (Control System)
Impact: Low
Security Controls: IA-6
References: NIST SP 800-53, NIST SP 800-82

Control system interfaces must be configured to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/ use by unauthorized individuals. Applicable STIG/SRG guidance for relevant components must be applied.

CRYPTOGRAPHIC MODULE

Applicability: (Control System)
Impact: Low
Security Controls: IA-7
References: NIST SP 800-53, NIST SP 800-82

From NIST SP 800-53: "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."

Not all cryptographic modules will require authentication and it is likely that there will be no such modules in the vendor's system. Modules requiring authentication are used only in the cryptographic protection of certain types of sensitive information. If such a module must be incorporated into the system, refer to any relevant STIG/SRG guidance or consult the customer as to a suitable implementation approach.

RE-AUTHENTICATION

Applicability: Application, (Control System)
Impact: Low
Security Controls: IA-11
References: NIST SP 800-53, NIST SP 800-82

The customer will determine if and under what conditions user re-authentication is required for the system. The technical mechanisms for enforcing re-authentication will be system specific. Re-authentication requirements should not conflict with availability needs of the AM system.

3.8 IR – Incident Response

Incident Response family controls ensure the organization has a formal procedure in place for handling system security incidents. These controls also require definitions for incident monitoring, reporting, and integration with other security processes such as configuration management, contingency planning, and personnel training. These controls are handled at the organizational level and are largely inherited from DoD-level or component-level policy.

3.9 MA – Maintenance

CONSIDERATION FOR MAINTENANCE PROVIDERS

Applicability: Application, (Control System)
Impact: Low
Security Controls: MA-2, MA-3, MA-4, MA-5, MA-6
References: NIST SP 800-53, NIST SP 800-82

Details of vendor maintenance activities on behalf of the customer will be specified by contractual obligations. RMF requires the organization to have a procedure for documenting all scheduled maintenance, repairs, replaced components, and completed maintenance. The organization must have policies and procedures for controlling the use of maintenance hardware and software tools, nonlocal maintenance processes, qualifications and clearances of maintenance personnel, and scheduling of timely maintenance to support system availability requirements.

3.10 MP – Media Protection

Media Protection family controls govern the handling, marking, and disposal of system media.

MEDIA SANITIZATION

Applicability: Printer
Impact: Low
Security Controls: MP-6
References: NIST SP 800-53, NIST SP 800-88

When a system or system components are decommissioned, RMF requires the organization to sanitize storage media in accordance with the requirements of NIST SP 800-88. This NIST special publication outlines methods for clearing, purging, and destroying different kinds of media and devices. The method selected depends on the sensitivity of the data contained and organizational policy. Clearing the printer by performing a reset to factory defaults may be determined sufficient if the printer never processed sensitive information. The more thorough alternative would be destruction. For smaller devices, the organization may elect to destroy the entire device, but this may prove difficult for larger machines. In either case, the vendor may assist the customer by providing recommendations for printer decommissioning in system documentation or service consultation. This information should include a description of all storage media in the printer, including ROM devices, and instructions for how to identify and remove them.

MEDIA USE

Applicability: Printer
Impact: Low
Security Controls: MP-7
References: NIST SP 800-53

The printer may allow for printing or system maintenance tasks to be performed from data in removable storage media. The vendor should clearly state any uses of removable storage media in system documentation. It should also be documented if and how the use of removable storage media may be disabled on the printer so that the customer may take appropriate actions, either through system configuration or compensating physical security controls, if this is deemed an unacceptable risk.

3.11 PE – Physical and Environmental Protection

Controls for Physical and Environmental Protection are meant to safeguard people, systems, and building infrastructure from any physical threats. These controls cover things like electricity, emergency shutoff, lighting, physical access control, fire prevention, and water damage protection. Aspects of security and safety in the physical operational environment of the system; these controls are handled at the organizational level and will generally be inherited from installation-level policy.

3.12 PL – Planning

The Planning control family ensures that the organization documents its requirements for providing, among other things, a security plan, a security concept of operations, security architecture document, and rationale for security control selection. These controls are handled at the organizational level and are largely inherited from DoD-level and component-level policy. The vendor supports these efforts indirectly through providing system documentation but does not draft these portions of the security plan if supplying only the printer and software components. If the contractor is providing or operating for the government customer a complete control system, then the contractor will need to provide the security concept of operations and security architecture document for the system as a whole, the requirements of which are outlined in more general guidance.

3.13 PM – Program Management

The formal management and implementation of the system information security plan is defined by the Program Management control family.

The critical infrastructure plan, information security plan, plan of action and milestones, risk management strategy, mission statement, and enterprise architecture are among the components of the system security plan developed in accordance with these controls. Controls for program management are handled organizationally and are inherited from DoD- or component-level policy. Depending on the details of the acquisition, the vendor may be required to submit drafts for a number of RMF artifacts containing system-specific information and supply the narrative for the system architecture description.

3.14 PS – Personnel Security

The controls for Personnel Security include instructions on how to safeguard the organization's employees through personnel screening, termination, transfers, access agreements, sanctions, and position risk.

The organizational level is responsible for managing personnel security controls, which are inherited from DoD- or component-level policy. For physical access to the printer and software (i.e., maintenance), a contract between the vendor and the organization is required.

3.15 PT – PII Processing and Transparency

The PII Processing and Transparency control family provides measures for the protection of Personally Identifiable Information.

These controls ensure organizational compliance with federal laws and regulations regarding privacy of individuals and requirements for PII handling. PII Processing and Transparency controls are handled at the organizational level and are inherited from DoD- and component-level policy.

3.16 RA – Risk Assessment

The Risk Assessment control family focuses on the risk assessment methods and vulnerability scanning capabilities of the organization. This control family is primarily handled at the organizational level.

VULNERABILITY SCANNING

- **Applicability:** Printer, Application
- **Impact:** Low
- **Security Controls:** RA-5
- **References:** NIST SP 800-53, NIST SP 800-82

Vulnerability scans of different kinds are performed routinely throughout the system lifecycle to ensure implementation of controls, aid in control assessments, and to support continuous monitoring activities. System scans automate the procedure for finding system and network configuration errors and identifying the presence of known vulnerabilities listed in dedicated databases. Almost all federal systems require ACAS (Nessus) scans and SCAP scans be performed for RMF activities. Other scan suites may be employed for specific system types as appropriate. The range of methods employed by these scanning techniques ranges from ping and open port scans to remote access of operating system files in credentialed procedures. Vulnerability scans designed for IT networks have historically caused difficulties in ICS networks. The vendor should always test and ensure that the printer is not adversely affected by common scans performed on its network – no persistent loss of availability, corruption of information, or aberrant behaviors during or after the scan. The customer may insist the printer should itself be scannable through credentialed (remote access to operating system files) procedures, in which case the vendor will have to figure out how to accomplish this with the limited computing resources in the printer controller.

3.17 SA – System and Services Acquisition

The System and Services Acquisition control family places the acquisition process under formal organizational control.

These controls are handled at the organizational level and are largely inherited from DoD- and component-level policy. Requirements for this control family will govern, in part, the contractual obligations the customer will place upon the vendor during a purchase or deployment. Delivery of vendor product documentation is required to fulfill SA-5.

3.18 SC – System and Communications Protection

System and Communications Protection family controls formalize measures to ensure confidentiality and integrity of data stored and transmitted by the system.

SEPARATION OF SYSTEM AND USER FUNCTIONALITY

- **Applicability:** Printer
- **Impact:** Moderate
- **Security Controls:** SC-2
- **References:** NIST SP 800-53, NIST SP 800-82

Separation of system management and user functionality entails either a physical or logical separation and is largely a matter of design choices that best support the unique requirements of the system. For the vendor, it is first necessary to determine what system management functions are supported by the printer and the application. Direct access to the printer OS, software, and configuration files would certainly fall under this category. Restricting this access though the use of a credentialed secure shell (SSH) terminal only used during maintenance would address the intentions of this control. Providing an administrative portal for printer configuration on the control workstation that requires elevated privileges to run could also serve to separate system and user functionality.

For the application, access to configuration settings that affect greater system behavior should be restricted to system administrative personnel with elevated privileges. This includes things such as networking settings and printer or device registration/authentication.

This control directly complements the separation of duties and least privilege controls from the access control family. Whereas the AC controls formalize these notions in organizational policy, this control addresses the technical measures to support them. As such, the vendor must make considerations for this control with a view towards how the printer and application are intended to be deployed within the customer's ICS.

INFORMATION IN SHARED RESOURCES

- **Applicability:** Printer
- **Impact:** Moderate
- **Security Controls:** SC-4
- **References:** NIST SP 800-53, NIST SP 800-82

Shared resources define a broad category that includes registers, processor caches, pages in main memory, files, directories, and file shares. If designed improperly, a system can "leak" information, such that one user's processes can read information from another user's processes when the resources used by these processes are deallocated to the system. All applicable STIG/SRG guidance for this control should be applied if possible. This control does make an important exception for system components that support only a single user or role. For a printer that operates a single service account to automatously receive and process print jobs, the risk of unintended transfer of information between system users via shared resources within the printer is negated and complies with the intent of this control.

During development of the application, the vendor should ensure industry best practices are followed for freeing memory and filesystem access during application code review.

DEFAULT NETWORK BEHAVIOR

- **Applicability:** Printer, Application
- **Impact:** Moderate
- **Security Controls:** SC-7(5), SC-10
- **References:** NIST SP 800-53, NIST SP 800-82

The printer should be configured to only allow and respond to the network ports and protocols necessary for its operation. It is best to simply ignore all other traffic.

All TCP connections and application protocol sessions should be terminated between the printer and application when the communication session is complete or after an inactivity timeout expires.

TRANSMISSION CONFIDENTIALITY AND INTEGRITY

- **Applicability:** Printer, Application
- **Impact:** Moderate
- **Security Controls:** SC-8, SC-8(1)
- **References:** NIST SP 800-53, NIST SP 800-82

Broadly speaking, confidentiality of transmitted information is supported by physical security of the transmission medium and/or encryption. Integrity is ensured by mechanisms used by the communication protocol, such as checksums, hashes, etc.

It is highly recommended that the vendor ensures all communication between the application and printer use protocols that incorporate transport layer security (TLS). In certain types of remote deployments, IPSec can be used to provide an additional layer of confidentiality protection. In addition to the selection of a communication protocol stack, the vendor can incorporate encryption and cryptographic integrity checks at the application layer within the application and printer software.

SYSTEM CRYPTOGRAPHY REQUIREMENTS

Applicability: Printer
Impact: Low
Security Controls: SC-12, SC-13
References: NIST SP 800-53, NIST SP 800-82

The requirements for cryptographic algorithms and modules used by the system are dictated by the sensitivity of the data residing on the system. The vendor should consult with the customer as to the types of sensitive information the system must be designed to handle. FIPS-validated (by FIPS 140-2 and 140-3 as of the time of this writing) algorithms and modules are a common requirement across federal systems. A list of FIPS-validated modules is published by the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/projects/cryptographic-module-validation-program).

It is not trivial to prove the use of FIPS-validated cryptography on a system. The vendor must ensure that current validated modules are installed on the system and then determine that the software components in the system are using the validated modules. Different software components handle this configuration item differently, and do not always exhibit a consistent behavior in this regard.

Note that there are other legal and regulatory requirements for cryptography for certain types of sensitive information. The DoD requires the use of National Security Agency (NSA)-approved cryptography for protection of classified information.

PROTECTION OF INFORMATION AT REST

Applicability: Printer
Impact: Moderate
Security Controls: SC-28
References: NIST SP 800-53, NIST SP 800-82

Information at rest is contrasted with information in transit (information being transferred between endpoints over a communication network) and information in use (information active in the processor or main memory). This state of information may be roughly considered as all system data that resides on nonvolatile system storage that at a given time is not being actively processed or transmitted. The organization is responsible for enacting mechanisms to protect first the confidentiality and secondly the integrity of the information at rest.

As the printer is not intended to be the primary locus of data storage in the ICS network, the vendor may elect to keep all print files in main memory during operation. In this case, special provisions for the protection of data at rest would not be applicable to the printer. Integrity checks of the data transmitted to the printer, such as file checksums, are still necessary but fall under a different set of security controls. In this type of deployment, print job batch control would be handled by the application on a server or workstation, which would apply the appropriate data at rest protection in accordance with STIG/SRG guidance.

If the printer design does feature secondary storage, protection of information at rest can be provisioned through FIPS-compliant whole-disk or filesystem encryption. A variety of hardware and software solutions exist to accomplish this encryption. The vendor will need to research which solutions are practical for their printer hardware and operating system. STIG guidance for related operating systems may provide a starting point for this research.

Cryptographic protection for data at rest should only be incorporated if the computational overhead does not adversely affect printer operating speed or responsiveness, as availability remains the overriding concern for ICS systems. If whole-disk or filesystem encryption cannot be applied to the printer, the system may be made compliant by compensating physical security controls. This would need to be communicated in system documentation.

PROCESS ISOLATION

Applicability: Printer
Impact: Low
Security Controls: SC-39
References: NIST SP 800-53, NIST SP 800-82

Modern multitasking operating systems load and execute each running process in a unique *virtual address space* such that each process is agnostic to the actual underlying physical memory layout and other running processes. All interprocess communication is handled by the OS according to the standard mechanisms provided by the OS. Containerization and virtualization techniques are enhanced forms of process isolation in which additional aspects of the execution environment may be abstracted from running processes.

Process virtual address space is an integral feature of most production multitasking operating systems. The OS developer documentation may be consulted to review and configure specific details of process memory allocation to best support the printer's operation, but in general process isolation should be implemented by default in the OS production configuration. When writing software for the printer, the vendor should internally track the use of interprocess communication mechanisms and review the software code to ensure that these are implemented in accordance with documented best practices. One caveat to the preceding discussion is that specific care should be taken when developing a kernel module or driver for the printer where the process isolation protections for userspace do not necessarily hold. Since printer software is specifically designed to control hardware, the need for a custom kernel-space driver may be quite possible during product development. The vendor should follow best practices in OS developer documentation for drivers and kernel extensions to ensure that memory from other processes is not accessed or modified.

Process isolation is a considerably more pertinent issue for *real-time operating systems* (RTOS), which are designed for minimal overhead and highly time critical embedded applications. For the purposes of this document we limit ourselves to the assumption that the controller within the printer itself uses a production-grade multitasking OS. The printer may however be integrated with real-time components in the industrial setting. We note that process isolation and general memory protection requires a completely different approach for RTOS's.

3.19 SI – System and Information Integrity

System and Information Integrity family controls enforce protections against unauthorized alterations to the system.

FLAW REMEDIATION

Applicability: Printer, Application
Impact: Low
Security Controls: SI-2
References: NIST SP 800-53, NIST SP 800-82

Unless explicitly specified in contractual obligations, it falls to the vendor to determine the development and release cycle of updates and patches to their printer and application. The vendor may determine how best to distribute patches and updates to their customers but must indicate this clearly in documentation and must never require that any device connect to the open internet to receive patches or updates. The vendor should abide by the details of any service agreements with the customer for system maintenance if this is included in the system acquisition.

The nature of industrial control systems prohibits as frequent patching as for IT systems. Some types of ICS cannot be effectively patched or updated. A well-designed control system should always include compensating measures to minimize the risk associated with older software versions. This is most effectively accomplished through network isolation.

The vendor may perform automated scans and manual checks for software components with identified vulnerabilities in the printer installation image. A number of tools and techniques for secure software development and potential vulnerability identification for the application are available to the vendor. The application software development SRG provides helpful guidance for software development security.

MALICIOUS CODE PROTECTION

Applicability: Printer
Impact: Low
Security Controls: SI-3
References: NIST SP 800-53, NIST SP 800-82

ICS computer components are required to employ malicious code protection mechanisms such as antivirus/antimalware software. This kind of software should not be necessary to be installed on the printer controller, but the customer may need to supply an exception waiver in their RMF package. Antivirus and antimalware definitions are updated frequently. Since ICS components should not directly communicate with the open internet, special consideration for updating definitions should be made, either as a recurring manual installation or provisioned through the ICS DMZ.

SYSTEM MONITORING

- **Applicability:** Printer, Application
- **Impact:** Low
- **Security Controls:** SI-4
- **References:** NIST SP 800-53

The organization should implement a procedure for continuous monitoring of the system for any abnormalities. This could be achieved through a variety of tools and techniques, including intrusion detection and prevention systems, scanning tools, and audit record monitoring.

SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

- **Applicability:** Printer
- **Impact:** Moderate
- **Security Controls:** SI-7
- **References:** NIST SP 800-53

Integrity checks may be performed by the system itself or by an external tool. Mechanisms including parity checks, cyclical redundancy checks, cryptographic hashes, and digital signatures may be used to detect unauthorized changes to software and data. Implementation details will be system specific. The operating system can provide checks of system programs, drivers, libraries, and regular files. Boot firmware can perform checks of operating system images prior to loading.

INPUT VALIDATION

- **Applicability:** Application
- **Impact:** Moderate
- **Security Controls:** SI-10
- **References:** NIST SP 800-53

Input validation is the procedure of examining user input received by the application to see whether it adheres to a standard set out in the application. It is the responsibility of the vendor to ensure that only valid inputs are accepted in the software application which prevents malicious code attacks. The vendor should confirm that the application is capable of handling input errors gracefully and provide informative error messages that does not reveal sensitive information. The application should be designed to maintain the integrity of the data as is being transferred.

Firmware updates can introduce new features and functionality but can also introduce security vulnerabilities. The vendor should ensure that all firmware updates are tested and free of invalid inputs thoroughly before deployments.

FLAW REMEDIATION

- **Applicability:** Printer, Application
- **Impact:** Moderate
- **Security Controls:** SI-11
- **References:** NIST SP 800-53

Organizations are required to ensure that error messages or notifications do not contain information that can be used to exploit the system when system errors invariably occur and that error message contents are viewed only by authorized personnel. While it is conceptually obvious that an information system should not be configured to openly advertise that it has certain set of vulnerabilities, enumerating the sheer variety of potential exploitable vulnerabilities that the system may be subject can make an exhaustive review of error messages for actionable information a challenging undertaking in practice. Since known system vulnerabilities should already be mitigated anyway, this compounds the difficulty of the task by requiring that unknown vulnerabilities be anticipated as well. For AM developers, there are practical measures that can be incorporated into the product design that can help gaining organizations comply with this control.

One measure is to divide error messages into two classes; a class of general messages for the standard user to indicate that an error occurred and a class of technical messages accessible only to privileged users, such as in a log file. Information to relegate to privileged users includes system state information, IP and port numbers, process and file names, memory dumps or usage statistics, and function or program offsets where faults or exceptions occur.

MEMORY PROTECTION

- **Applicability:** Printer
- **Impact:** Moderate
- **Security Controls:** SI-16
- **References:** NIST SP 800-53

NIST defines memory protection as hardware-enforced or software-enforced mechanisms to prevent execution of code residing in regions of memory designated as non-executable. Most modern operating systems allocate system memory to processes in standard-sized blocks called *pages*. Pages allocated to running processes are tracked in one or more *page tables*, depending on the details of the operating system implementation. The majority of processor architectures recognize a flag applied to entries in the page table generally called a “no execute” bit and will fault if a program attempts to execute machine instructions in this page of memory. Operating systems are responsible for setting the “no execute” bit when allocating memory to processes. This is handled by a program called the executable file interpreter or loader when a program is initiated and will set the “no execute” bit for all loaded program segments except those designated as program text in the executable file. All dynamic (runtime) memory allocations will be

prohibited from being executed by userspace processes in most operating systems.

Another mechanism for memory protection is *address space layout randomization*. Most multitasking operating systems provide userspace processes a *virtual address space* in which to execute. This has the practical benefit of being able to compile programs that are agnostic to their actual layout in physical memory at runtime and has a security benefit of isolating processes from the memory of other processes. In a virtual address space, a process only "sees" itself and the operating system in memory. The kernel keeps track of translating the process' virtual address space to physical memory allocations. By applying levels of randomization between the virtual and physical memory offsets, certain kinds of memory overflow attacks (i.e. techniques to overwrite executable sections of memory, such as the stack) are made considerably more difficult.

Memory protection techniques are a fundamental aspect of operating system security. In practice, almost all modern production operating systems will incorporate these techniques by default. Considerations for memory protection are more pertinent for embedded system developers engineering specific, purpose-built OS installations. Memory protection mechanisms always incur a small but constant performance overhead that must be taken into account. The benefits in a multitasking system far outweigh this cost, however, so there is no suitable justification to omit them except in the most critical of real-time applications. The AM developer must ensure that full memory protection is configured to the extent supported by their selected hardware and OS. Implementation of memory protection techniques varies between processors and operating systems, so the AM developer must consult the product documentation to learn the full extent of their capabilities. Any configuration rules for SI-16 should be enacted if a DISA STIG exists for the selected or a similar OS distribution for the printer.

3.20 SR – Supply Chain Risk Management

Supply Chain Risk Management controls formalize the organization's approach to verifying the trustworthiness of vendors and products throughout the supply chain.

These controls are handled at the organizational level in accordance with DoD-wide and component-level guidance. Although the vendor does not directly handle the supply chain risk management for their customer, the vendor can expect to provide information at the customer's request in fulfillment of these controls. This will be included in the vendor's contractual obligations.

Anti-tamper technologies and techniques are covered in this control family. Vendors wishing or required to include anti-tamper mechanisms in their product may reference the ISO 20243 standard.

4 Approaches to Cybersecurity Compliance Documentation

Approaches to Cybersecurity Compliance Documentation

The Risk Management Framework is one of a number of cybersecurity frameworks, each with a considerable overlapping scope of requirements as well as distinct application-specific focuses. RMF is primarily of interest because it is the framework that federal entities, including the DoD and its components, are mandated to utilize.

The proliferation of complementary frameworks, however, testifies to the reality that the holistic nature of cybersecurity makes securing a system and its data irreducible to any single compliance checklist. When it comes to cybersecurity of a system, there is a fundamental distinction between implementation and compliance. The latter is meaningless without the former, that is, without first putting effective security measures in place. For the vendor, no compliance framework can serve as a substitute for engineers, programmers, and program managers keenly knowledgeable about the product's inner workings and how security measures may be best applied. These authors recommend a best practice for vendors to internally catalogue and track cybersecurity risk management for their product and translate this information into the cybersecurity framework for their customers. This document primarily introduces the technical requirements imposed by RMF for what may be expected in an average DoD ICS. This set of security measures may ultimately neither be considered a sufficient set or even a necessary set of security measures appropriate for the printer and application, but must be addressed at some level if the vendor expects to conduct business with DoD entities. One way or another, each of the system level controls must be demonstrated to implement the intent of the control, be mitigated through another compensating mechanism, or be truly not applicable to the secure operation of the system.

The vendor's task beyond delivering the AM product is effectively and accurately communicating the security status of the system to the customer. How this is accomplished is dependent on the details of the product acquisition. Different types of acquisitions may be categorized as direct or indirect acquisitions. An indirect acquisition would occur if a federal entity or contractor purchased the AM product as a commercial-off-the-shelf (COTS) purchase with no unique contractual requirements for product development or modification. In this scenario, the vendor has no contractual obligations to produce artifacts for RMF, so the means of communicating product cybersecurity are limited. System documentation is the primary source of information for the customer here and should include a detailed product configuration and deployment guide. The headings in the previous section will be of interest to the customer for RMF purposes. A table mapping product security features to RMF controls can be a helpful addition to product documentation or promotional material. Publishing a whitepaper covering product cybersecurity may also be an effective way to educate prospective customers. Finally, the highest level of product security assurance that a vendor may advertise is in identifying, applying, and, if possible, receiving a third-party certification for a recognized commercial cybersecurity standard for their product.

Obligations to produce RMF artifacts and documentation may be included when the vendor is directly contracted by a DoD entity to provide an AM system. These obligations may also be included in subcontracts. The documentation required for a DoD RMF package is listed in DI-MGMT-82001A. The vendor may be asked to contribute a subset of these documents. When submitted to the customer, these documents are only drafts as the package must be finalized by the system owner. A set of representative RMF artifact templates are included as attachments to this document for reference purposes. However, the vendor should always request authorized templates from the customer if available. These should include the eMASS Implementation Plan and Test Results bulk upload forms as well.

As the preceding section demonstrates, much of the RMF policies and procedures must originate from the customer's organization. The vendor is only expected to supply the information pertaining to their contribution to the system. The vendor should request a Risk Management Framework Knowledge Service (RMFKS) export for the AM system control selection from the customer (or information for how to access RMFKS themselves). The RMFKS information will list both DoD Tier 1 and Component Tier 2 implementation guidance. This will provide the vendor with the definitive control selection for the system as well as all relevant DoD CCI-level requirements at the same time.

When drafting artifacts, it is imperative for the vendor to write the documents for the customer's use and not conflate the vendor's own cybersecurity policy into the customer's documentation. The customer will assess the vendor's cybersecurity practices through other contractual mechanisms. These should be referenced wherever the RMF controls deal with the vendor's security compliance.

This document only contemplates the security measures appropriate for the printer and the control application, as authoritative guidance already exists for other ICS components. The vendor should be aware that if supplying the printer and application as components of a larger control system, they must comply with the existing guidance for the other system components, which is external to the scope of this document.

The approach to RMF artifact generation should be methodical and done in regular consultation with the customer. The following is a recommended course of action for preparing the RMF artifacts as defined by DI-MGMT-82001A during the acquisition lifecycle.

At the beginning of the project, the intended AM control system should already be given a security categorization with a selected control baseline and overlays. The RMF Implementation Plan, listing all of the selected controls for the system, can be developed right from the start of the project. If the customer has already registered the system in eMASS, this can be exported and shared with the vendor. A Test Results export may be obtained at this time for future use.

- Implementation Plan
- Test Results

When the design of the system has been completed, whether at the beginning of the project or after a designated design phase, a number of security plan elements can be derived.

- **System Information** – a high-level overview of what the system is and does
- **Mission Description** – a statement of how the system supports its intended mission
- **System Concept of Operations** – brief description of how the system is intended to be used
- **Operating and Computing Environment** – the intended operating environment and the way in which the system is intended to interact with other systems
- **Physical Security Measures** – summary of the physical protection measures used by the customer, if available
- **Facilities Descriptions** - description of the customer's facility where the system will be deployed, if available

These security plan elements are intended to be relatively short summaries. The customer will indicate whether these are to be included as parts of a single security plan document or as separate deliverables. Ultimately, these will be used to fill the corresponding forms in eMASS.

At this time there should be a good idea of what system components will be used in the system so a list of applicable STIGs and SRGs can be compiled. As a corollary, the Information Assurance Test Plan, which lists the STIGs/SRGs to be applied to the system as well as the types of scans and other test methods for compliance, may be produced also. The IA Test Plan should also include instructions for how to conduct the tests for the system, spelling out any needed hardware/software/network reconfigurations, system states, or user privileges to ensure successful tests.

- STIG/SRG List
- IA Test Plan

It may also be decided following system design what user types will be authorized for the system and the necessary clearances for these types. If the customer agrees on a set of user types for the system, these may be listed at this time. Otherwise, these sections may be left for the customer to complete. A set of generic user types may be suggested, such as general user, system administrator, and system auditor. RMF security roles or positions may already be designated for customer personnel and should be listed if available. Designation of these roles is not guaranteed to be completed during the vendor's involvement in the acquisition process. Certain RMF roles may be filled by personnel outside of the customer's immediate organization.

- User Descriptions and Clearances
- Security Roles

As the system is being installed on location, specific technical information may be compiled and included in RMF template formats. If only certain system components are being purchased, the vendor is only responsible for the components they are contracted to provide. At this stage, the following security plan elements may be drafted.

- **System Architecture Description** – detailed narrative of the system contents
- **Compliant Network Diagrams** – graphical representation of system components and network connections between them, drawn in accordance with customer-specified formats. The network diagrams can also relay the following information:
    - Authorization Boundary – will be defined formally earlier in the project as all of the system components subject to the provisions of the security plan, but should be represented unambiguously in the system diagrams
    - External Interfaces and Data Flow – should be clearly represented in the diagrams. Data flow indicates the types and attributes of information exchanged between components and the direction of flow (e.g. application data, network protocol, encryption type, etc.). May also be described in a narrative. Data flow also includes,
      Internal Data Flow – i.e. between system components in the authorization boundary, as opposed to external connections
- **Hardware/Software/Firmware Lists** – spreadsheet listings of all hardware, software, and firmware components in the system with version information, manufacturer, and system location
- **Ports, Protocols, and Services List** – list of all network protocols, open TCP/UDP ports, and network services used in the system. Although typically restricted to IP based communication, it is conventional for ICS to include a list of non-IP based communications as well, if these are present.
- **System Configuration** – all system configuration files should be copied and saved separately from the system after it is complete and security hardened. This includes the registry and GPO's from Windows OS's, /etc directory contents for Unix-like OS's, and managed switch configuration files. A manifest of these files is to be included in the security plan.

The vendor will typically be required to verify system cybersecurity hardening prior to handover to the government customer in the form of scan results and STIG/SRG checklists.

- **Scans** – results of automated systems scans, namely ACAS/Nessus and SCAP scans identified previously in the IA Test Plan, should be delivered to the customer in their original format and represent the actual state of the system at handover.
- **STIG/SRG Checklists** – the system must be checked for compliance with identified applicable STIGs and SRGs. This may be done manually but it is preferable to use an automated tool (SCAP scan) to the greatest extent possible. Results are to be delivered as STIG checklist files, which may be viewed and created with the DISA STIGViewer application.

When the pertinent information for the system has been gathered, the remaining documentation for the RMF package may be completed. Whereas the artifacts mentioned up to this point almost certainly require the vendor's expert knowledge of their system, much of the rest of the RMF package reflects the customer's internal policy. The following procedure for producing the next set of artifacts is recommended below.

- **Test Results (Completed)** – a spreadsheet format list of all applicable assessment procedures / CCIs for the system and the compliance status of each. This document serves as the most comprehensive and granular view of overall system compliance of all other artifacts. Attention should be directed to the relevant portions for the vendor. CCIs referenced in applied STIGs should be identified and marked in the test results. CCIs designated as "technical" type should be given the most attention and are usually prefaced with "the information system…" as opposed to the "the organization…" in the CCI text. Policy CCIs directly related to the technical CCIs in the same control may also be marked. Each assessed AP / CCI should be designated as "compliant" or "non-compliant," as the case may be, with a brief description of how this is demonstrated. For CCIs the vendor cannot determine, these may be designated as "not assessed." The Test Results export may already include inherited CCIs as compliant.
- **Standard Operating Procedures (20 control families)** – SOP's are integral artifacts of the system security plan containing the narratives that detail policy, procedures, and technical measures taken by the organization for each selected control. There is usually one SOP for each control family. The contractor should focus their efforts on controls implemented by the system and allow the gaining organization to address matters of their own policy. Appendix A is provided as an approximation of what controls are affected by vendor system choices, but the exact list will vary in the course of an actual acquisition. Control narratives should address all the CCI statements for that control. The narratives should reference the guidance documents used to shape policy.
- **Implementation Plan (Completed)** – a listing of the compliance status of all selected controls. It is recommended that the Implementation Plan be completed for the vendor-provided drafts after the assessment Test Results. Although this is somewhat the reverse of the formal RMF procedure, it allows for the Implementation Plan to be completed unambiguously. Each control is given an "implementation status" and a "security control designation." If all CCIs are inherited for a control, the security control designation is "common"; if some but not all, "hybrid"; if none, "system-specific." If all CCIs for a hybrid or system specific control are compliant, the implementation status is "implemented." If it is a common control, then its status is "inherited." If a control does not have all CCIs compliant, it is not fully implemented, and its status is "planned." If the control pertains to a functionality that the system does not possess, the control may be designated, with the agreement of the customer, as "not applicable." Controls with different status must be supplied with additional information. Common controls must indicate the common control provider. Not applicable controls must have a justification of why the control is considered not applicable. Implemented controls must have an implementation narrative, which may be summarized from the SOP's. Additional information for the Implementation Plan will be provided by the customer.
- **Plan of Action and Milestones** – a listing of all non-compliant CCIs at the time of handover with a description of the non-compliance issue, planned remediation actions, timeframe for these actions, and personnel or entities responsible. The non-compliant and not assessed CCIs from the assessment Test Results may be collected and entered into a customer-approved format for the POAM. It is important to designate which CCIs are considered non-compliant because these must be handled by customer policy (and thus will become compliant with the enaction of such policy) and those non-compliant because an actual technical measure was not applied (e.g. an open STIG rule that could not be addressed for some reason). The contractor may leave the sections for the timeframe of corrective actions and personnel involved for the customer to complete.

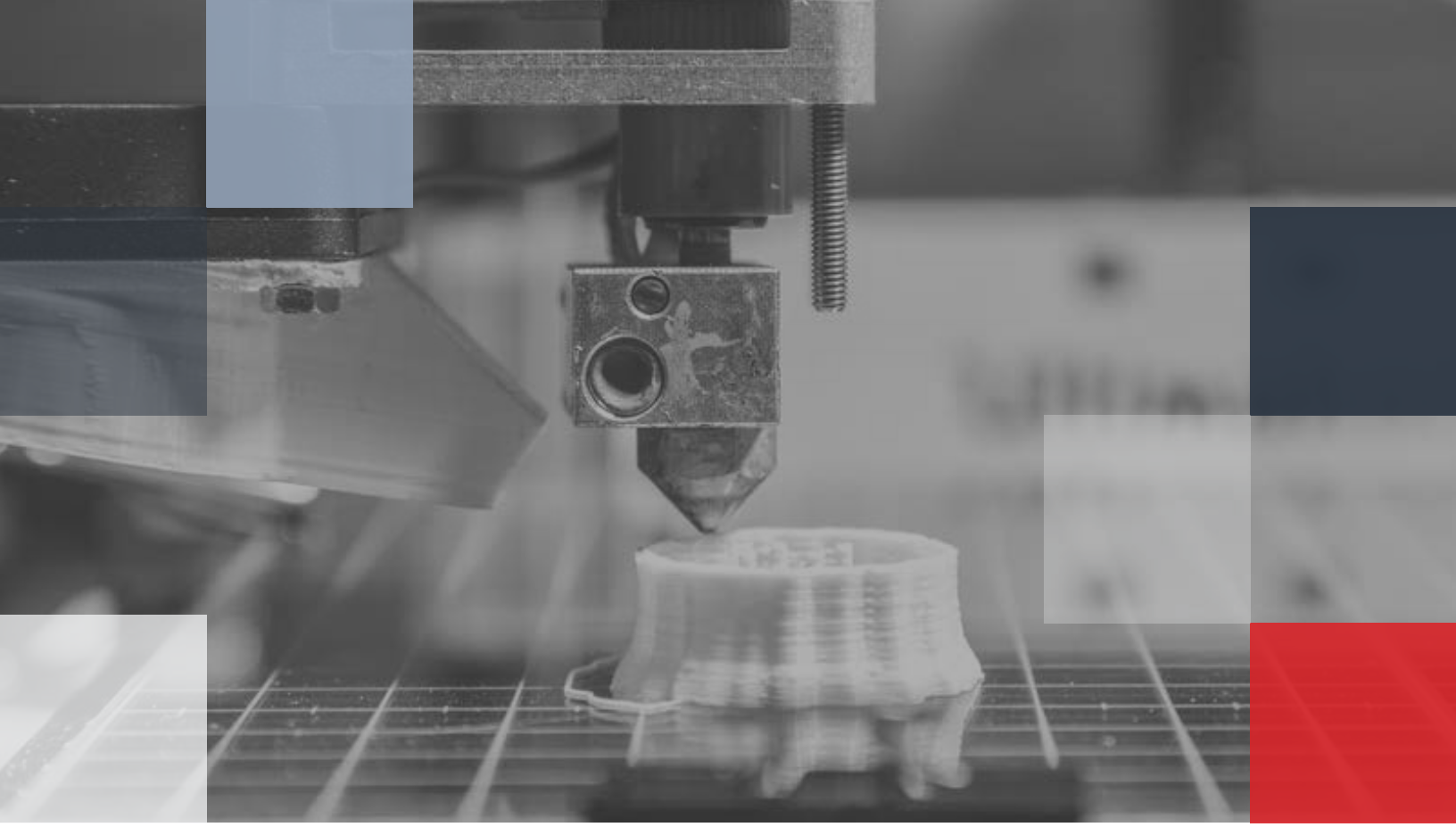
The RMF system security plan contains several subordinate plans described here. The vendor may be asked to provide details or narrative sections for how to accomplish certain relevant procedures for their system.

- **Contingency Plan** – a plan detailing the organization's procedure for continuity of operations and ensuring the system's mission following a security compromise or catastrophic loss.
- **Configuration Management Plan** – a plan for how changes made to the system will be placed under formal organizational control.
- **Incident Response Plan** – a plan detailing actions to be taken in the event of a security incident, including containment measures, forensic investigations, and after action reports.
- **Information Assurance Vulnerability Management Plan** – a plan for the approach the organization will take to identify system vulnerabilities and apply flaw remediation.

The remaining DI-MGMT-82001A documents deal with assessment and authorization procedures or are situational. These have little bearing on the vendor and are not elaborated upon here. Further clarification from the customer should be requested if the vendor is asked to contribute to these.

5

Vendor Cybersecurity Responsibilities During the DoD Acquisition Lifecycle



Vendor Cybersecurity Responsibilities During the DoD Acquisition Lifecycle

The major Responsible-Accountable-Supportive-Consulted-Informed (RASCI) activities for stakeholders in the DoD acquisition lifecycle are summarized in Annex B of the *DoD Program Manager's Guidebook for Integrating the Cybersecurity RMF into the System Acquisition Lifecycle*. The reader is directed to this publication for details of RMF in the DoD acquisition process. In this section an exposition is given for the activities identified for the system developer / integrator in the RASCI table.

The role of the system developer / integrator as contemplated in the DoD acquisition process definitions is a general one that includes either a government or private entity. The vendor, as a government contractor, will not have input to the acquisition process prior to the publication of the RFP and the drafting of the acquisition contract. The vendor's input into the initial system cybersecurity design will also be finalized before the system owner's request for ATO. Therefore, the RASCI activities for a private contractor during initial acquisition exclude the activities identified prior to Milestone B and after Milestone C of the formal DoD acquisition process and are not considered in this document. Certain activities outside of this window may on occasion be included in contract language, particularly if the program office considers it appropriate for supplier contribution in refinement of the cybersecurity requirements. The customer will clarify these specific requests. Note that post-ATO sustainment activities have been excluded from this discussion to restrict the scope of the document to acquisition activities prior to handover. The system security plan undergoes regular updates during the course of sustainment after ATO is granted. The vendor should be aware of their supportive role should their contract extend to provide services during sustainment. The content and scope of the RMF security plan and artifacts do not change at this time, however, so the approach given in the previous section would still apply.

All contract deliverables, including RMF package deliverables, will be given a data item description in the contract data requirements list (CDRL) with the relevant authoritative reference indicating the expected contents and format for each deliverable. It is the vendor's responsibility to ensure the traceability of cybersecurity requirements throughout all relevant contract deliverables.

Major developer activities during EMD are described below. Official definitions of all DoD acquisition lifecycle activities are given in the *Defense Acquisition Guidebook*.

RESPONSIBLE

Engineering and Manufacturing Development (EMD) Phase (Annex A-3)

Characterize the attack surface and begin to assess cybersecurity in planning and performing component and system integration testing.

The vendor must generate and submit an attack surface characterization document detailing all possible methods for malicious or deleterious actions to the system. The Guidebook defines the attack surface as, "The attack surface defines the system's exposure to reachable and exploitable vulnerabilities, to include any hardware, software, connection, data exchange, service, removable media, etc., that might expose the system to potential threat access." An attack surface characterization is thus an enumeration of all potential attack vectors. Using a formal framework such as the *MITRE Corporation Adversarial Tactics, Techniques & Common Knowledge* (MITRE ATT&CK®) knowledge base is highly recommended for characterizing the attack surface as methodically and comprehensively as possible.

Complete the detailed build-to design of the system, ensuring that cybersecurity requirements are included.

The detailed, production-level design of the system will be communicated through several contract deliverables. The vendor must ensure that this documentation references the system cybersecurity requirements where appropriate. Cybersecurity requirements are defined by the security controls and other authoritative guidance from the DoD and its subordinate entities. Any documentation describing the system computer hardware, software, or network will almost certainly need to reference cybersecurity requirements.

Conduct systems engineering, including technical planning as defined in the approved SEP, and verify compliance with the functional, allocated, and product baselines.

The vendor will need to detail their approach to system security engineering in the System Engineering Plan (SEP). Requirements for system security engineering are discussed in Section 6 of this document.

Ensure that cybersecurity requirements are mapped and allocated to the hardware and software design.

Throughout this document, there has been a focus on security control requirements as they relate to AM system components. During the acquisition, the vendor will be required to map the requirements to the components of the control system formally in the design documentation. The goal is to provide clear traceability between the cybersecurity requirements and the design features.

SUPPORTIVE

EMD Phase (Annex A-3)

Critical Design Review

The vendor will provide a supportive role in the Critical Design Review. The activities of this review are described in chapter 3-3.3.5 of the *Defense Acquisition Guidebook*.

Develop Security Assessment Plan (SAP) in support of the Interim Authorization to Test (IATT) application. Provide to the Authorizing Official.

Submit draft Security Authorization Package at IATT in order to conduct system testing activities.

IATT must be obtained if a system not yet granted ATO must be deployed in an operational environment for testing purposes. If required, an IATT Request will be submitted to the AO with the IA Test Plan along with possibly other RMF package artifact drafts. The vendor supports this effort by drafting of the RMF package artifacts as described in Section 4 of this document.

Conduct developmental test and evaluation (DT&E) event to demonstrate system maturity and readiness to begin production and preparedness for operational test and evaluation and/or deployment and sustainment activities.

Prepare DT&E assessment as input to Milestone C Decision.

The vendor supports system test and evaluation activities during the EMD phase as directed by the customer.

Functional Configuration Audit

System Verification Review

Production Readiness Review

The vendor supports these reviews by supplying the required system information in conjunction with testing and evaluation prior to the Milestone C decision.

ACCOUNTABLE

The DoD Program Manager's Guidebook does not designate the role of Developer or System Integrator as "Accountable" for any of the identified RMF activities during the DoD system acquisition lifecycle. The Guidebook defines this responsibility as, "Role ultimately accountable for the work. Individual with final decision authority, or depending on the product, signatory authority." Accountability for RMF activities will generally fall upon administrative roles within the program office.

CONSULTED

EMD Phase (Annex A-3)

Map and allocate cybersecurity requirements to the hardware and software design for the system as part of the overall system development process and to support test and evaluation planning.

Cybersecurity requirements traceability is necessary for the generation of system test and evaluation plans.

Ensure that Critical Design Review (CDR) entrance criteria for cybersecurity baseline design are met and that all cybersecurity requirements are reflected in the product baseline, which includes the design.

Cybersecurity requirements traceability must be included in product design deliverables going into Critical Design Review.

Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection. (prior to CDR) Update TSN analysis focused on system-level functions, including CA to identify critical functions, TA, VA, TSN Risk Assessment, and countermeasure selection. (prior to Milestone C)

The TSN analysis is conducted in accordance with DoDI 5200.44 *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*. This analysis includes a Criticality Analysis (CA), Threat Assessment (TA), Vulnerability Assessment (VA), Risk Assessment (RA), and countermeasure selection and application. These are updated several times during the acquisition lifecycle, including prior to CDR and prior to Milestone C, following Functional Configuration Audit.

INFORMED

EMD Phase (Annex A-3)

Assess the system using appropriate procedures to determine the extent to which the controls are effective, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Prepare a Security Assessment Report (SAR) against the Security Assessment Plan.

Performed after CDR and prior to IATT Request submittal.

Conduct vulnerability analysis and testing to evaluate the system's cybersecurity in a mission context using realistic threat exploitation techniques.

Performed after IATT Request and prior to developmental test and evaluation.

Conduct Vulnerability and Penetration Assessment that includes overt, cooperative, and comprehensive examination of the system to characterize the system's operational cybersecurity status.

Conducted prior to Functional Configuration Audit.

6

System Security Engineering Considerations

System Security Engineering Considerations

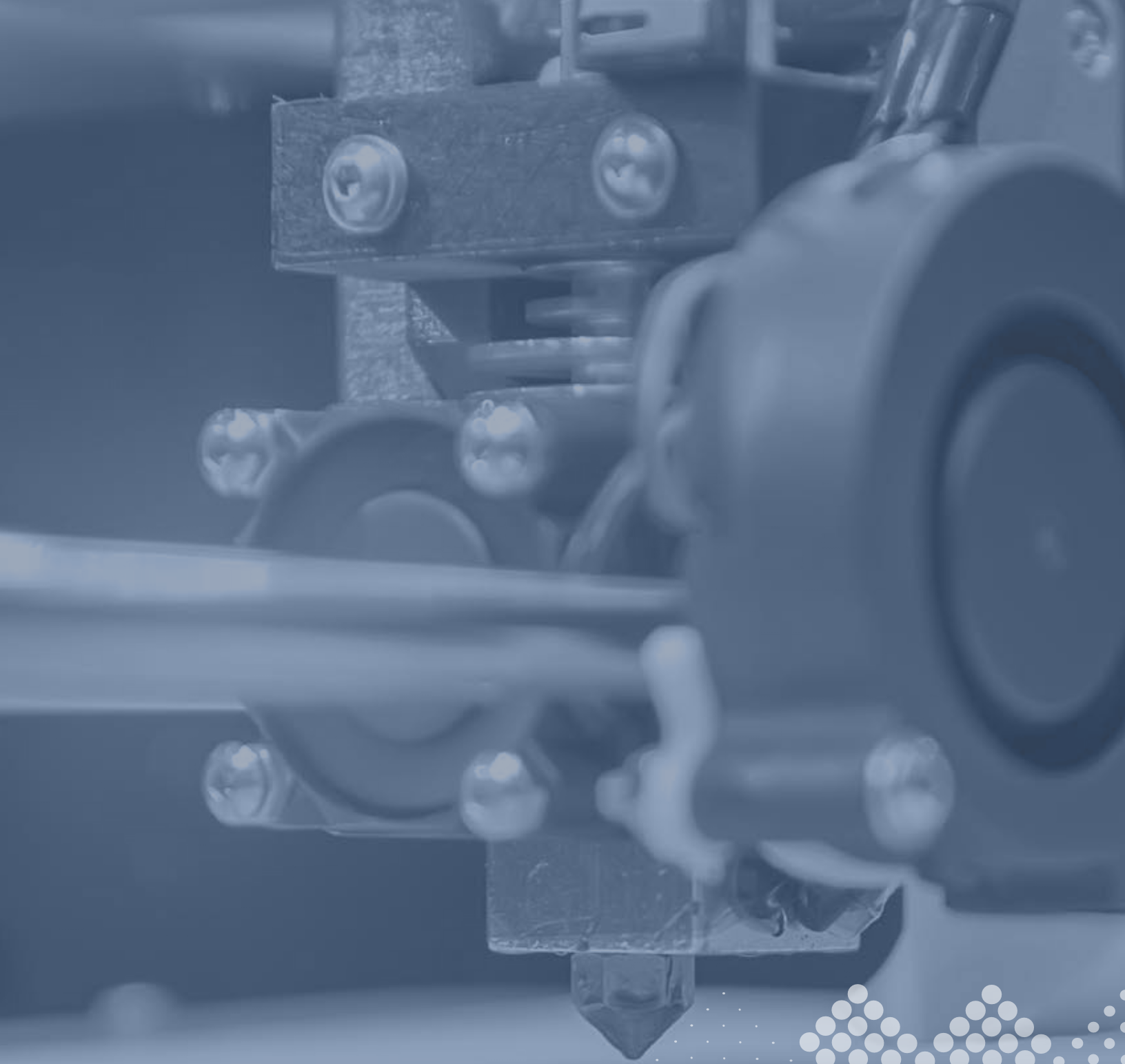
Systems engineering for DoD systems is to be conducted in accordance with DoDI 5000.88. A DoD-wide reference outline for the Systems Engineering Plan (SEP) is published by the Office of the Deputy Director for Engineering and is accessible at, https://ac.cto.mil/engineering.

System security engineering considerations in the SEP are driven by the program protection plan (PPP) drafted by the program office. The PPP is created in accordance with the guidelines in DoDI 8000.53.

A formal approach to systems security engineering is provided in the NIST SP 800-160, which comprises two volumes. NIST SP 800-160v1, *Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, defines a systems engineering framework consisting of high-level system life-cycle *processes* and security design *principles*. The NIST SP 800-160v1 processes cover aspects of system security engineering as a whole and are appropriate for use to guide either engineering activities during a DoD acquisition process or as an internal development process for the vendor. The processes are general in scope and may be applied to AM system components individually or as an integrated whole. Many of the processes share similar objectives to RMF controls, however, the overall focus is different. RMF provides a picture of system security from an operational standpoint, whereas NIST SP 800-160v1 views it from a development standpoint. Still, RMF control requirements can be used to drive system life-cycle process activities and provide a means to trace system design elements back to cybersecurity requirements.

The security design principles listed in Appendix F of NIST SP 800-160v1 provide a basis for the attributes that secure system design should incorporate.

NIST SP 800-160v2, *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, is used as companion guidance to NIST SP 800-160v1 and NIST SP 800-37. This publication outlines a framework for developing cyber resiliency - taking proactive measures to incorporate cybersecurity into product design. The framework presented is intended to assist developers in translating high-level security design goals and objectives to actionable techniques and design principles. NIST SP 800-160v2 encourages developers to tailor their security design approach to meet the unique needs of their system and provides specific advice for a variety of system types that are not traditional enterprise IT systems. Guidance for cyber-physical and internet-of-things (IoT) systems will likely be of interest to AM developers.



7 References

References

- Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 2016.
- OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017.
- OMB Memorandum 02-01; Guidance for Preparing and Submitting Security Plans of Actions and Milestones, October 2001.
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006.
- OMB Memorandum M-11-33, FY2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, September 2011.
- Committee on National Security Systems Instruction 1253, Security Categorization and Control Selection for National Security Systems, September 2017.
- Department of Defense Instruction (DoDI) 5000.88, Engineering of Defense Systems, November 2020.
- DoDI 8500.01, Cybersecurity, March 2014.
- DoDI 8510, Risk Management Framework (RMF) for DoD Information Technology (IT), July 2017.
- DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, May 2015.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995.
- NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments, July 2002.
- NIST SP 800-37, Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011.
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002.
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.
- NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, December 2014.
- NIST SP 800-59, Guideline for Identifying an Infor mation System as a National Security System, August 2003
- NIST SP 800-60, Revision 1, Revision 2 Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004.
- NIST SP 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, August 2008.
- NIST SP 800-82, Guide to Operational Technology (OT) Security, April 2020.
- NIST SP 800-88, Guidelines for Media Sanitization , December 2014.
- NIST SP 800-100, Information Security Handbook: A Guide for Managers, March 2007.
- NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011.
- NIST SP 800-160 Volume 1, Engineering Trustworthy Secure Systems, November 2022.
- NIST SP 800-160 Volume 2, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, December 2021.
- NIST SP 1800-32B, Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity, February 2022.
- US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts.

8/9 Appendices

8 Appendix A: RMF Control Applicability Matrix

The controls for which the AM machine manufacturer/vendor are partially responsible for implementation in a DoD deployment are listed in the table below. The "Implementation" column is taken from NIST SP 800-53r5 and indicates whether the control is implemented via organizational policies and procedures, "O", system configuration and design considerations, "S", or a mixture of both. The "Impact" column indicates whether the control is included in the low (LLL) or the moderate (MMM) security control baseline for system confidentiality, integrity, and availability (CIA). All low impact controls are included in the moderate selection. The remaining columns indicate which controls the manufacturer/vendor are responsible, in part, for supporting and broadly the manner in how they are supported. The designations have been applied to two broad categories in accordance with the industry standard of how system control functionality is divided in a typical deployment. The "printer" is defined as the AM machine hardware, firmware, operating system, drivers, libraries, and specialized control software residing within the machine enclosure. The "application" is the software interface that relays information to and from the AM machine. This application may be installed on an onsite control workstation or be part of a remote/cloud deployment. The software that handles direct communication with the AM machine will often be integrated with a suite of programs that handle various aspects of AM manufacturing control and design. All manufacturer/vendor software that is installed on hardware components in the system scope are considered the "application" collectively.

In these columns, the symbol "A" indicates an administrative or policy control, implemented by the gaining organization, which is supported by the manufacturer/vendor in the form of system documentation, consultation, or fulfillment of various other contract requirements during acquisition. The symbol "X" indicates a configuration setting or design feature that must be applied to the system to meet the intent of the control, or mitigated through other technical means. The applicability of a number of controls in the list are affected by several factors described below.

[1] – Applicable only to devices with a full local user interface. A full local user interface is implemented directly by the device and supports user accounts with configurable privileges requiring a logon to access device data and settings. Some devices may support a minimal local user interface that does not provide configurable accounts. For a minimal local user interface, only a subset of these controls may be applicable and are specified in the control guidance section of this document. Security controls for a remote user interface would be handled by the application.
[2] – Applicable only to devices with wireless network connectivity.
[3] – The processing capabilities of the AM machine controller determine the level of audit logging that may be required.
[4] – Device authentication may be applicable at different OSI levels, depending on the system architecture.
[5] – Applicability depends upon overall system architecture. In general, access control and authentication would only be handled by the application for certain types of distributed/cloud deployments. Otherwise, these controls would be implemented by the host operating system or network/domain.

Controls applied to other types of system components that may be included in the system scope of an actual deployment, such as control workstations or network infrastructure, have been excluded from consideration as authoritative information security guidance for these types of components is provided elsewhere.

No.	Control ID	Control Name	Implementation	Impact	Printer	Application
1	AC-2	Account Management	O	LOW	A	A
2	AC-2(3)	DISABLE ACCOUNTS	S	MODERATE	X [1]	X [5]
3	AC-2(4)	AUTOMATED AUDIT ACTIONS	S	MODERATE	X [1]	X [5]
4	AC-2(5)	INACTIVITY LOGOUT	O/S	MODERATE	X [1]	X [5]
5	AC-3	Access Enforcement	S	LOW	X	X
6	AC-4	Information Flow Enforcement	S	MODERATE	X	X
7	AC-6	Least Privilege	O	MODERATE	A	A
8	AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS	S	MODERATE	X [1]	X [5]
9	AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	S	MODERATE	X [1]	X [5]
10	AC-7	Unsuccessful Logon Attempts	S	LOW	X [1]	X [5]
11	AC-8	System Use Notification	O/S	LOW	X [1]	X [5]
12	AC-11	Device Lock	S	MODERATE	X [1]	X [5]
13	AC-11(1)	PATTERN-HIDING DISPLAYS	S	MODERATE	X [1]	X [5]

No.	Control ID	Control Name	Implementation	Impact	Printer	Application
14	AC-12	Session Termination	S	MODERATE	X [1]	X [5]
15	AC-17	Remote Access	O	LOW	A	A
16	AC-17(1)	MONITORING AND CONTROL	O/S	MODERATE	X [1]	X [5]
17	AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	S	MODERATE	X [1]	X [5]
18	AC-18	Wireless Access	O	LOW	A	A
19	AC-18(1)	AUTHENTICATION AND ENCRYPTION	S	MODERATE	X [2]	
20	AC-18(3)	DISABLE WIRELESS NETWORKING	O/S	MODERATE	X [2]	
21	AU-2	Event Logging	O	LOW	A	A
22	AU-3	Content of Audit Records	S	LOW	X [3]	X
23	AU-3(1)	ADDITIONAL AUDIT INFORMATION	S	v	X [3]	X
24	AU-4	Audit Log Storage Capacity	O/S	LOW	X [3]	
25	AU-5	Response to Audit Logging Process Failures	S	LOW	X [3]	
26	AU-8	Time Stamps	S	LOW	X [3]	
27	AU-9	Protection of Audit Information	S	LOW	X [3]	
28	AU-12	Audit Record Generation	S	LOW	X [3]	X
29	CM-2	Baseline Configuration	O	LOW	A	A
30	CM-6	Configuration Settings	O/S	LOW	X	X
31	CM-7	Least Functionality	O/S	LOW	A	A
32	CM-7(2)	PREVENT PROGRAM EXECUTION	S	MODERATE	X	
33	CM-7(5)	AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION	O/S	MODERATE	X	
34	CM-8	System Component Inventory	O	LOW	A	A
35	CP-9	System Backup	O	LOW	A	A
36	CP-10	System Recovery and Reconstitution	O	LOW	A	A
37	IA-2	Identification and Authentication (Organizational Users)	O/S	LOW	A	A
38	IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	S	LOW	X [1]	X [5]
39	IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	S	LOW	X [1]	X [5]
40	IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT	S	LOW	X [1]	X [5]
41	IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS	S	LOW	X [1]	X [5]
42	IA-3	Device Identification and Authentication	S	MODERATE	X [4]	X [4]
43	IA-4	Identifier Management	O	LOW	A	A
44	IA-5	Authenticator Management	O/S	LOW	X [1]	X [5]
45	IA-5(1)	PASSWORD-BASED AUTHENTICATION	O/S	LOW	X [1]	X [5]
46	IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION	S	MODERATE	X [1]	X [5]
47	IA-6	Authentication Feedback	S	LOW	X [1]	X [5]
48	IA-7	Cryptographic Module Authentication	S	LOW	X [1]	X [5]
49	IA-11	Re-authentication	O/S	LOW	X [1]	X [5]
50	IR-6(3)	SUPPLY CHAIN COORDINATION	O	MODERATE	A	A
51	MA-2	Controlled Maintenance	O	LOW	A	A
52	MA-3	Maintenance Tools	O	MODERATE	A	A
53	MA-4	Nonlocal Maintenance	O	LOW	A	A

No.	Control ID	Control Name	Implementation	Impact	Printer	Application
54	MA-5	Maintenance Personnel	O	LOW	A	A
55	MA-6	Timely Maintenance	O	MODERATE	A	A
56	MP-6	Media Sanitization	O	LOW	A	
57	MP-7	Media Use	O	LOW	A	
58	PE-9	Power Equipment and Cabling	O	MODERATE	A	A
59	RA-5	Vulnerability Monitoring and Scanning	O	LOW	A	A
60	SA-4	Acquisition Process	O	LOW	A	A
61	SA-5	System Documentation	O	LOW	A	A
62	SA-8	Security and Privacy Engineering Principles	O	LOW	A	A
63	SA-10	Developer Configuration Management	O	MODERATE	A	A
64	SA-11	Developer Testing and Evaluation	O	MODERATE	A	A
65	SC-2	Separation of System and User Functionality	S	MODERATE	X	
66	SC-4	Information in Shared System Resources	S	MODERATE	X	X
67	SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION	S	MODERATE	X	
68	SC-8	Transmission Confidentiality and Integrity	S	MODERATE	X	X
69	SC-8(1)	CRYPTOGRAPHIC PROTECTION	S	MODERATE	X	X
70	SC-10	Network Disconnect	S	MODERATE	X	X
71	SC-12	Cryptographic Key Establishment and Management	O/S	LOW	X	X
72	SC-13	CRYPTOGRAPHIC PROTECTION	S	LOW	X	X
73	SC-17	Public Key Infrastructure Certificates	O/S	MODERATE	X [1]	X [5]
74	SC-23	Session Authenticity	S	MODERATE	X	X
75	SC-28	Protection of Information at Rest	S	MODERATE	X	
76	SC-28(1)	CRYPTOGRAPHIC PROTECTION	S	MODERATE	X	
77	SC-39	Process Isolation	S	LOW	X	
78	SI-2	Flaw Remediation	O	LOW	A	A
79	SI-3	Malicious Code Protection	O/S	LOW	A	
80	SI-4	System Monitoring	O/S	LOW	A	A
81	SI-7	Software, Firmware, and Information Integrity	O/S	MODERATE	X	
82	SI-7(1)	INTEGRITY CHECKS	S	MODERATE	X	
83	SI-10	Information Input Validation	S	MODERATE		X
84	SI-11	Error Handling	S	MODERATE	X	X
85	SI-16	Memory Protection	S	MODERATE	X	
86	SR-6	Supplier Assessments and Reviews	O	MODERATE	A	A
87	SR-8	Notification Agreements	O	LOW	A	A
88	SR-12	Component Disposal	O	LOW	A	A

9 Appendix B: RMF Artifact Templates

- Contingency Plan Template
- Incident Response Plan Template
- Hardware / Software List Template
- Plan of Action and Milestones Template
- Ports, Protocols, and Services List Template
- RMF Control Family SOP Templates

MD Cyber

PLAYBOOK SERIES

www.mxdusa.org/cyber