Cyber Security – A Vendor Perspective

ZODIAC DATA SYSTEMS

ZODIAC AEROSPACE

Bob Baggerman
Zodiac Data Systems

Cyber Security Motivation for Vendors

- **Customers won't procure equipment that doesn't meet cyber security requirements**

- **Broad range of customers, not just DoD**
  - Commercial – Boeing, Airbus, Gulfstream, others
  - DoD – All Services

- **<u>ALL</u> customers are concerned about Cyber Security**

Cyber Security is a procurement discriminant

Cyber Security Challenges for Vendors

- Vendors may not understand customer requirements
- Customers may not understand customer requirements
- Little specific guidance from the DoD
- Vendors don't have access to resources
  - rmfks.osd.mil
  - eMASS
- Vendors are not part of the requirements process
  - Impact assessment (Low, Medium, High)
  - Control Inheritance
  - Security Authorization Package

Vendor Role in Cyber Security

- **Implement a Cyber Secure organization**
  - Cyber Security is more than just a secure product
  - Cyber Security is a secure organization
- **Be Prepared to Prove It**
  - Appropriate cyber security hardening and testing
  - Documented RMF Control compliance

Equipment can’t be used without Approval To Operate

Understanding the Approval Process – Begin with the end in mind

Authorizing Decision Document (ATO or IATT)

Transmits the final security authorization decision from the AO or AODR to the information system owner or common control provider and other key organizational officials, as appropriate

- **Authorizing Official (AO) or the Authorizing Official Designated Representative (AODR) signs based on risk assessment from the Security Authorization Package (SAP)**
  - Aircraft - Dr. Kalabhai “Raju” Patel
  - Weapons – Mr. George Mooney
- **Contains the following information:**
  - Authorization decision
  - Terms and conditions for the authorization
  - Authorization termination date
  - Risk executive (function) input (if provided)

Understanding the Approval Process – Begin with the end in mind

Security Authorization Package

Documents the results of the security control assessment and provides the AO with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls.

- **Security Plan (SP)**
- **Security Assessment Report (SAR)**
- **Plan of Action and Milestones (POA&M)**
- **Authorization Decision Document**
  - Authorization To Operate (ATO)
  - Initial Authorization To Test (IATT)

Understanding the Approval Process – Begin with the end in mind

Security Plan

- Provides an overview of the **security requirements** and describes the **RMF security controls in place** or planned for meeting those requirements
- Provides sufficient information to understand the **intended or actual implementation** of each security control employed within or inherited by the information system.
- NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems
  - "System Boundary Analysis and Security Controls"
  - "System Security Plan Development"

Customers need help documenting security controls in RMF terms

Risk Management Framework (RMF)

- **RMF is the methodology to assess vulnerabilities and ultimately risk**
- Considers
  - Effectiveness
  - Efficiency
  - Constraints
- Must take into account
  - Applicable laws
  - Directives
  - Executive Orders
  - Policies
  - Standards
  - Regulations.

RMF Process – Controls

Security Controls

- RMF Controls are a Component of Security Plan
- NIST SP 800-37 *Guide for Applying the Risk Management Framework* provides the top level guide
- FIPS 200 provides 17 broad categories of security controls
- Further break down of controls
  - NIST SP 800-53 – Baselines based on the overall security impact
  - CNSS 1253 – Better Granularity
- NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* defines detailed baseline security controls for various system impact levels
- NIST SP 800-53A *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* is the companion to 800-53 and provides further guidance

RMF Process – Controls

Family ID	Control Family Name	Number of Controls	Number of Enhancements
Security Controls:			
AC	Access Control	23	89
AT	Awareness and Training	4	6
AU	Audit and Accountability	16	42
CA	Security Assessment and Authorization	8	14
CM	Configuration Management	11	39
CP	Contingency Planning	12	36
IA	Identification and Authentication	11	45
IR	Incident Response	10	24
MA	Maintenance	6	20
MP	Media Protection	8	14
PE	Physical and Environmental Protection	19	31
PL	Planning	6	4
PS	Personnel Security	8	7
RA	Risk Assessment	5	8
SA	System and Services Acquisition	20	66
SC	System and Communications Protection	41	75
SI	System and Information Integrity	16	66
Privacy Controls:			
AP	Authority and Purpose	2	0
AR	Accountability, Audit, and Risk Management	8	0
DI	Data Quality and Integrity	2	3
DM	Data Minimization and Retention	3	3
IP	Individual Participation and Redress	4	2
SE	Security	2	0
TR	Transparency	3	2
UL	Use Limitation	2	0
Program Management Controls:			
PM	Program Management	16	0

Broad Categories (from FIPS 200)

Example – SA-12 Supply Chain Protection

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization **protects against supply chain threats** to the information system, system component, or information system service by employing [*Assignment: organization-defined security safeguards*] as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance: Information systems (including system components that compose those systems) need to be **protected throughout the system development life cycle** (i.e**., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement**). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to **educate the acquisition workforce on threats, risk, and required security controls**. Organizations use the acquisition/procurement processes to **require supply chain entities to implement necessary security safeguards** to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. **Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system**. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.

Example – SA-12 Supply Chain Protection

- SA-12(1) SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS
- SA-12(2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS
- SA-12(3) SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING
- SA-12(4) SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS
- SA-12(5) SUPPLY CHAIN PROTECTION | LIMITATION OF HARM
- SA-12(6) SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME
- SA-12(7) SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE
- SA-12(8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE
- SA-12(9) SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY
- **SA-12(10) SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED**
- SA-12(11) SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS
- SA-12(12) SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS
- SA-12(13) SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS
- SA-12(14) SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY
- SA-12(15) SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES

Example – SA-12 Supply Chain Protection

SA-12(10) VALIDATE AS GENUINE AND NOT ALTERED

The organization **protects against supply chain threats** to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.

Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, **distribution**, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the **identification, management, and reduction of vulnerabilities** at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to **implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain**; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements.

Each control and enhancement reads like a small novel

RMF Process – Control Tailoring

RMF Process

- Step 1 - Categorize System
- **Step 2 - Select Security Controls**
  - Start with CNSSI 1253 controls based on impact
  - **Tailor for specific situation**
  - Apply community overlays (if any)
- **Step 3 - Implement Security Controls**
  - Document security control implementation in the security plan
- Step 4 - Assess Security Controls
- Step 5 - Authorize System
- Step 6 - Monitor Security Controls

Control tailoring has a major impact on cyber security requirements

RMF Process – Control Tailoring

Security Controls (Continued)

- Applicability for each security control is governed by a three by three matrix of impact for each security objective
  - From FIPS 199 Table 1
- Security Objective (CIA)
  - Confidentiality
  - Integrity
  - Availability
- Potential Impact
  - Low
  - Moderate
  - High

RMF Process – Control Tailoring

Security Controls (Continued)

- Example of CNSSI Security Control Baselines
  - From CNSSI 1253 Table D-1

ID	TITLE	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
AC-1	Access Control Policy and Procedures	X	X	X	X	X	X	X	X	X
AC-2	Account Management	X	X	X	X	X	X			
AC-2(1)	Account Management | Automated System Account Management		X	X		X	X			
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X	X		X	X			
AC-2(3)	Account Management | Disable Inactive Accounts		X	X		X	X			
AC-2(4)	Account Management | Automated Audit Actions	+	X	X	+	X	X			
AC-2(5)	Account Management | Inactivity Logout	+	+	X	+	+	X	+	+	X
AC-2(6)	Account Management | Dynamic Privilege									

What is a Vendor To Do?

- The government user produces all the documentation in the Security Authorization Package.
- We can greatly assist in this process by providing important information about how our equipment implements the necessary security controls.
  - **Tailoring for specific situation**
  - **Implementation of necessary controls**
- The challenge in our vendor role is that we don't know what RMF security controls are to going to be required by the AO or AODR.

Vendors should be prepared to describe cyber security of products expressed in terms of RMF controls

RMF Process – Which controls to implement and document

Some Important Controls

- CM-6 Configuration Settings
- CM-9 Configuration Management Plan
- CM-11 User installed software
- MP-1 Media Protection Policy and Procedures
- MP-2 Media Access
- MP-6 Media Sanitization
- MP-7 Media Use
- MP-8 Media Downgrading
- RA-5 Vulnerability Scanning
- SA-10 Developer Configuration Management
- SA-11 Developer Security Testing and Evaluation
- SA-12 Supply Chain Protection
- SA-18 Component Authenticity
- SI-7 Software, Firmware, and Information Integrity

RMF Process – Which controls to implement and document

- Many of our security controls will be **inherited**
  - Defined in NIST SP 800-37 and CNSSI 4009
- **Common Security Control -** “A security control that is inherited by one or more organizational information systems.”
- **Hybrid Security Control** - "A security control that is implemented in an information system in part as a common control and in part as a system-specific control."
- **Security Control Inheritance** - "A situation in which an IS or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."

Specific controls depend on customer requirements

RMF Process – Which controls to implement and document

Document Controls Already In Place

SA-12 SUPPLY CHAIN PROTECTION

SA-12(1) ACQUISITION STRATEGIES / TOOLS / METHODS

The organization employs the following processes for the purchase of the information system, system component, or information system service from suppliers.

- •Suppliers selection and management : IGA000004 Managing Suppliers
- •Procurement process : IGA000017 Purchasing Data
- •Purchase agreement in place for 60% of purchase value. Contracted include NDA. Standard contract defined by Zodiac Corporate for all the new contracts
- •NDA in place with the majority of other sub contractors and main suppliers

SA-12(2) SUPPLIER REVIEWS

The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service.

- •Suppliers selection and management : IGA000004 Managing Suppliers
- •Supplier preliminary questionnaire IMP000136 compliant to ZA-Q-1006
- •Requirement applicable to suppliers ZA-Q-1030

RMF Process – Which controls to implement and document

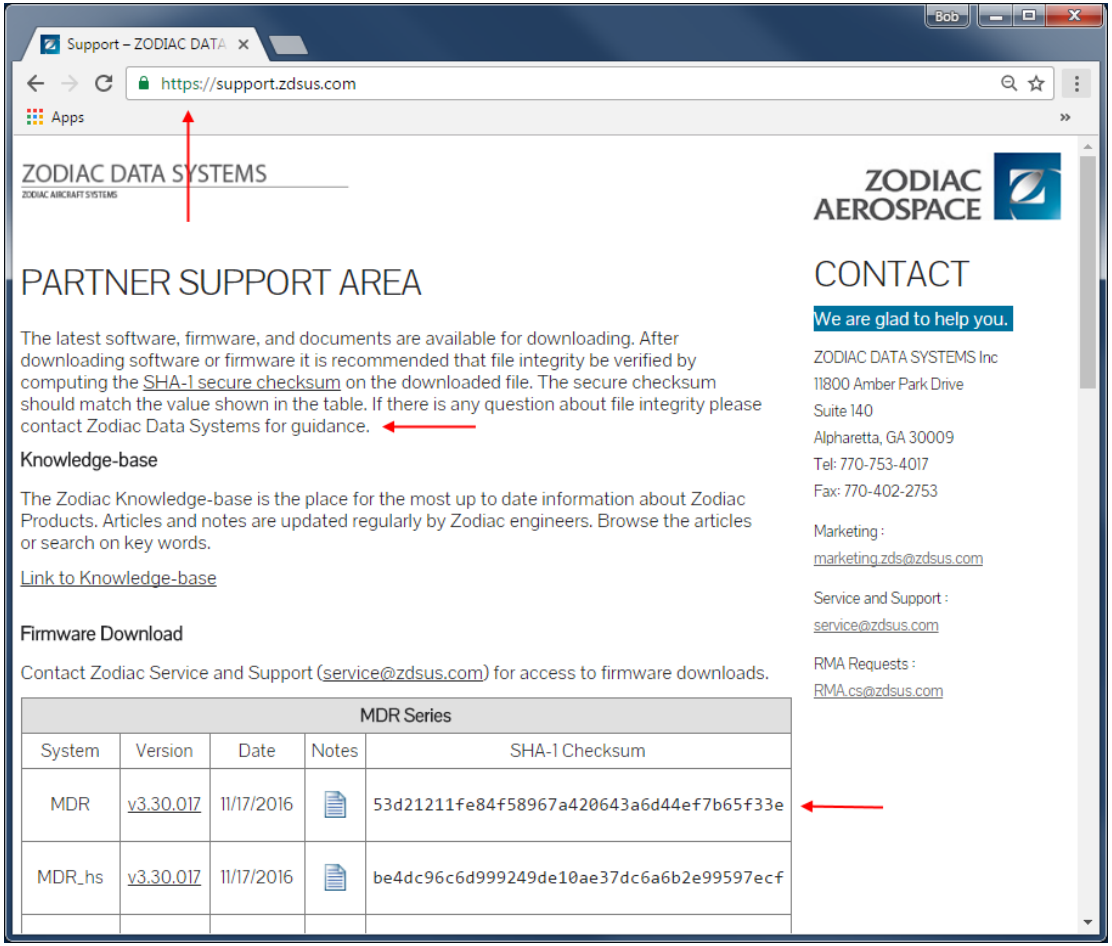
- Identify Gaps using Mission Based Risk Assessment
- Implement Improvements

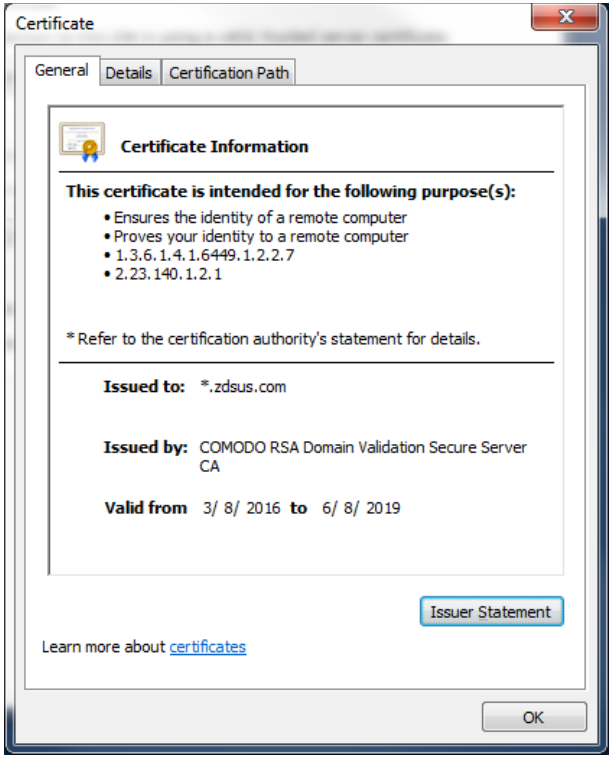
Example - SA-12(10) VALIDATE AS GENUINE AND NOT ALTERED

Firmware delivered electronically

Physical Control of Server
Secure web protocol HTTPS
Cryptographically signed
Cryptographic signatures available via separate channel

RMF Process – Which controls to implement and document





Summary

- **For Vendors**
  - Study and Understand RMF Process
    - RMF controls are not requirements!
  - Study and Understand Approval Process
  - Participate in Cyber Security Events
  - Anticipate Cyber Security Requirements
    - Perform a Mission Based Risk Assessment (Cyber Tabletop, etc.)
    - Implement Controls / Testing / Documentation
- **For DoD customer**
  - Need more and better RMF guidance from DoD
    - Overlays
    - Tailoring
    - Requirements
    - Inherited Controls
    - Priorities