A VENDOR PERSPECTIVE IN SUPPORT OF CYBERSECURITY OF (INSTRUMENTATION) SYSTEMS

Jeff Rusincovitch
Zodiac Data Systems, Inc.
Agenda

1. Background – Zodiac Data Systems, Inc.
2. Overview of Implementing RMF at ZDS
3. ZDS Product Lifecycle Threat and Risk Assessment Process
4. Comprehensive Security Review by Department of Security Services (DSS)
5. Summary
ZDS Product Lines

Market leader in two fields: Instrumentation & Space

Air & Space Systems

Tracking Ground Systems

INSTRUMENTATION
Flight Test

Data Acquisition Units & Recorders
Flight Termination Receiver

Tracking & Processing Ground Flight Test Station
Flight Termination Station

SPACE
Ground Solutions for Satellites & Launchers

No ZDS equipment on satellites
Tracking antennas
RF
Critical Modems

A UNIQUE VALUE PROPOSITION
Zodiac Data Systems, Inc.

■ 40 year legacy in Instrumentation and Telemetry

■ U.S. Regional / Responsive Expertise
  ▶ Expert Sales Force
  ▶ Local Field Application Engineers for product training/support/sales

■ Small business attached to large business resources
  ▶ Small business agility and customer connection
  ▶ Large engineering work force located in France and Germany

■ U.S. Entity with ability to work U.S. classified contracts
  ▶ Operating under Special Security Agreement (SSA)
  ▶ Structured and monitored by U.S. Defense Security Service
  ▶ Mitigates Foreign Ownership and Controlling Influence (FOCI)
ZDS Commitment to Cyber Security

- DFARS 252.204-7012
- Protect Covered Defense Information (CDI)
- ZDS compliant with NIST800-171
- Federal Information Security Management Act (FISMA)
- Protect Information Systems
- ZDS routinely supports Authorization to Operate (ATO)
- New focus area for U.S. Defense Security Services Audits for Cleared Defense Contractors
Overview of Implementing RMF at ZDS
RMF & Security Controls

- **NIST SP 800-37** Guide for Applying the Risk Management Framework

- **NIST SP 800-53** Security and Privacy Controls for Federal Information Systems and Organizations

- **Challenge:** Our products are used on a wide range of applications each with unique RMF, risk tolerance, common controls, etc.

- How do vendors proactively establish RMF and Security Controls that supports every customers’ needs?
Approach to Implementing Security Controls

- Lessons Learned from Supporting ATO
- Product Life Cycle Risk Assessments
- Product Penetration Testing
- Customer Requirements for Product Features
- Identify Security Control
- Security Control Documentation ‘Library’
- Process & Procedure Enhancements
- Product Enhancements
## Select Implemented Security Controls

<table>
<thead>
<tr>
<th>No.</th>
<th>Security Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA-3</td>
<td>Risk Assessments</td>
</tr>
<tr>
<td>CA-8</td>
<td>Penetration Testing</td>
</tr>
<tr>
<td>CM-9</td>
<td>Configuration Management Plan</td>
</tr>
<tr>
<td>RA-5</td>
<td>Vulnerability Scanning</td>
</tr>
<tr>
<td>SA-10</td>
<td>Developer Configuration Management</td>
</tr>
<tr>
<td>SA-12</td>
<td>Supply Chain Protection</td>
</tr>
<tr>
<td>SA-19</td>
<td>Component Authenticity</td>
</tr>
<tr>
<td>SI-12</td>
<td>Information Handling and Retention</td>
</tr>
<tr>
<td>SI-16</td>
<td>Memory Retention</td>
</tr>
</tbody>
</table>
Select Supporting Documents for Controls

- Detailed Statement of Volatility
- Statement of Safety for Databus Interfaces
- Vulnerability and Conformity Scans
- Firmware/Software/FPGA Development Policy
- Firmware Release Policy
- Supply Chain Protection Policy
- Prevention of Counterfeit Parts Policy
PRODUCT LIFECYCLE THREAT AND RISK MANAGEMENT

- Product Life Cycle Risk Assessments
- Product Penetration Testing
Product Lifecycle Risk Management

Focus Areas:
- From component sourcing to customer delivery
- Service and repair
- Firmware updates
- Typical components and interconnections for instrumentation system

Priority is to protect Confidentiality
3, 4) Adversary gains access to product to install malware\(^3\) or steal data\(^4\)

10) Adversary gains network access to steal data.
Threat and Risk Assessment Process

- Product Lifecycle Threat Events
- Risk Assessments (CTTs)
- Vulnerability Assessments (Pen Test)
- Plan of Action
  - Product Enhancements
  - Policy/Procedure Improvements
Approach to Implementing Security Controls

- Lessons Learned from Supporting ATO
- Product Life Cycle Risk Assessments
- Product Penetration Testing
- Customer Requirements for Product Features
- Identify Security Control
- Security Control Documentation ‘Library’
- Process & Procedure Enhancements
- Product Enhancements
Comprehensive Security Review by Department of Security Services (DSS), 2018
DSS Addressing Cyber Security Concerns

Moving Ahead

- National Industrial Security Program (NISP) designed for vastly different time
- Moving to an intelligence-led, asset-focused, and threat-driven approach that:
  - Prioritizes assets and facility engagement based on national intelligence information
  - Identifies assets at each cleared facility
  - Considers the threat and vulnerabilities
  - Partners with cleared industry to develop tailored security programs
Audit Focus – FPGA

- Functionality – purpose and functions of FPGA in device
- Suppliers – current vendors providing FPGAs
- Supply chain process – supplier management, risk management and component authentication
- Process integrity of firmware development
- Software toolsets used for firmware development
Audit Process

- Safeguards found to be in place to protect sensitive information
- ZDS is in compliance with NISPOM
- ZDS received favorable remarks for FPGA Supply Chain Integrity, Process Integrity and Software Toolset…BUT…
- Specific feedback not provided:
  - Threat source and events considered
  - Opportunities to improve vulnerabilities and controls
Summary
Summary

- ZDS is proactively managing cyber security of products and supporting customers achieve ATO

- Each application is different and vendors are challenged with anticipating security requirements

- Vendors need specific Cyber Security requirements from customers to effectively support ATO

- Vendors need ongoing support from customers security experts to understand emerging trends and threats
POWERED
BY TRUST