RMF In Action for Control Systems

Mr. Tim Nauman
AFCEC/COM
Facility Cybersecurity SME
The Early Days....

I did get better....

But it’s no match against Baba Yaga...
• RMF is a Risk Management Process for information assurance
• Requires
  – Risk Frame
  – Assess and Accredit Plan
  – Continuous Monitoring Strategy
  – Accreditation Authority
• Based on Roles and Responsibilities
RMF and Control Systems

- RMF applies to control systems
  - Utility Management & Control
  - Energy Management and Control
  - Local Control
  - Networked Control
  - Long-Distance SCADA
  - Micro grids
  - IP-Enabled Control Devices
RMF Staffing

• RMF requires people
  – Designated roles and responsibilities
  – With IA certifications
  – And ICS skills and experience
Responsibility for Risk Management

- Responsibilities are tied to system ownership
  - DoD Network Use
  - Ability and Authority to direct change
  - Resources to implement change
  - Responsibility for the system and its operational impact
- DoD Systems
  - DoDI 8510.01
  - NIST SP800-53
  - NIST SP800-82
  - Service Branch RMF Guidance
- Non-DoD systems serving the DoD
  - DFARS 252.204-7012
  - NIST 800-171
  - Additional Contract Requirements
## RMF Steps

<table>
<thead>
<tr>
<th>RMF Step</th>
<th>NIST SP800-171</th>
<th>NIST SP800-82</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categorize Information System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Select Security Controls</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Implement Controls</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Assess Controls</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Authorize Information Systems</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Monitor Controls</td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>
How to Support RMF

- Responsibilities to Support RMF Activities
  - DoD
    - Project Management
    - UFC application
    - Require involvement of the Receiving Organization
    - Stand-in for the Receiving Organization if needed
    - Be aware of the minimum document requirements at system acceptance
      - Risk Frame
      - System Engineering Plan
      - System Security Plan
      - POA&M
  - Energy Service Company
    - Provide documentation
    - Recognize that your SSP may require more detail
    - Prepare artifacts for key security decisions
    - Recognize that the customer may need helpful guidance
Questions?