DoD Cybersecurity Trends for Energy Systems

16 May 2017

Presented by:
Jay Kurowsky, President & CEO
256-895-8870
jay.kurowsky@aletatechnologies.com
Agenda

- Risk Management Framework Type Authorization
- DFARS/NIST Cybersecurity Compliance Requirements
- Control Systems Approved Products List
- Cloud Computing for Control Systems
Password= Roll Tide?  

1996

Shock and Awe?  

2003

Piece of “Cake”?  

Today

(no it’s hard, and we have to work hard)
Risk Management Framework (RMF)

**Step 1: CATEGORIZE System**
- Categorize the system in accordance with CNSSI 1253
- Initiate the Security Plan (SP)
- Register system with DoD Component IA Program
- Assign qualified personnel to RMF roles

**Step 2: SELECT Security Controls**
- Common Control Identification
- Select security controls and document SP
- Develop system-level continuous monitoring strategy
- Review and approve SP and continuous monitoring strategy

**Step 3: IMPLEMENT Security Controls**
- Implement control solutions consistent with DoD and Component IA architectures
- Document security control implementation in SP

**Step 4: ASSESS Security Controls**
- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

**Step 5: AUTHORIZE System**
- Prepare the POA&M
- Submit Security Authorization Package (SP, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

**Step 6: MONITOR Security Controls**
- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update SP, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

RMF Process for DoD IT Systems
Per DoD Instruction 8510.01 and other sources: “The type authorization is used to deploy identical copies of an IS or PIT system in specified environments. This method allows a single security authorization package to be developed for an archetype (common) version of a system. The system can then be deployed to multiple locations with a set of installation, security control and configuration requirements, or operational security needs that will be provided by the hosting enclave.”
Type authorization/accreditation has been around for decades (originally called generic accreditation).

A common historical usage of type accreditation is for weapons systems such as tanks or helicopters.

It is used to save money so that testing and assessment can be performed once and reused multiple times.

OSD and some of the Services are realizing that even if the system/environment is not identical, type authorization can save large amounts of money and schedule time.

OSD = Office of the Secretary of Defense
As used in the RMF, reciprocity is the acceptance of test assessment, and resulting artifacts created by one Service by the other Services.

OSD wants type authorization, and Air Force, Army, and Navy are currently working reciprocity issues.
Many smart control system manufacturers have recognized type authorization is coming and have begun the process.

Even though type authorization is not fully implemented for energy systems, artifacts are in high demand and create market advantage for manufacturers.
DoD grew tired of losing its sensitive information via cyber attacks to its soft commercial underbelly.

DoD has decided that it is no longer suitable for contractors to try to hide behind $100 Walmart firewalls—real security is needed.

Which of these designs came from the U.S? Apparently both.
DoD prescribed Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 for any covered contractor information system which processes, stores, or transmits covered defense information.

Covered Defense Information is defined within DFARS 252.204-7012 as “...Unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html [such as that information considered FOR OFFICIAL USE ONLY] that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is--marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.”
Compliance Requirements

- DFARS 252.204-7012 requires compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171
- SP 800-171 is similar to an abbreviated RMF process
- The deadline for compliance with DFARS 252.204-7012 is 31 December 2017

In the unlikely event that you don’t have to comply with DFARS 252.204-7012, I recommend you comply anyway since the process prescribes great ways to help prevent your company from being hacked, and who wants to be hacked???
Control Systems Approved Products List

- In addition to type authorization, OSD is looking toward a Control Systems Approved Products List as a way to save money and get secured energy and other control system products fielded more quickly.

- The concept is very similar to that of the longstanding Unified Capabilities Approved Products List (UC APL) that has been operated by Defense Information Systems Agency.

- Like UC APL, the concept is to use Federal Acquisition Regulation (FAR) Part 9.2 to have manufacturers pay to have their products and systems qualified for cybersecurity and other functions such as interoperability and functionality.
Cloud Computing for Energy Systems

Many energy manufacturers and ESCOs ask me about cloud computing, and here are the basics:

- Like pretty much anything else, cloud use is not impossible, you just need to figure out the rules, how to achieve your goals relatively securely, and how to get Government decision-makers to agree.

- A key “rule” to could computing is FedRAMP, which is somewhat like RMF for cloud service providers.

- At the current time, Microsoft Azure and CSRA/ARC-P are the only two FedRAMP-approved cloud offerings.
Another New Trend: More Emphasis on Old Trends

Per a recent Energy Services Performance Contract (ESPC) request for proposal:

“The government favors offerors that propose the utilization of appropriately qualified cybersecurity personnel (Information Security Systems Architects and Engineers) and explains the role of these personnel in this potential task order.”
On May 11\textsuperscript{th}, President Trump signed Executive Order titled \textit{Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure}

“...sitting by and doing nothing is no longer an option.”

- Thomas Bossert, White House Homeland Security Advisor speaking on President Trump’s new cybersecurity legislation
11 May Executive Order

- The Executive Order holds agency heads accountable for cybersecurity risk.

- It seems likely that the result of this executive order will be this, so the overall cybersecurity trend will be increasing requirements on manufacturers, ESCOs, and others doing business with DoD.
Conclusion

- A variety of new things are going on in the cybersecurity world that affect energy systems.
- Early adopters can gain market advantage.
- Even though some of these concepts will take a while to catch on, historical cybersecurity requirements and DFARS/NIST requirements are starting to get teeth.
Oh, by the way, as suggested for mention by the “Other Jay”

- **The National Cyber Summit**, an initiative of Energy Huntsville’s sister organization, Cyber Huntsville, will be 6-8 June at the Von Braun Center
  - Classified session on Day 1
  - Cyber Cup hacking competition
  - Numerous nationally-recognized speakers
  - Find out more and register at: www.nationalcybersummit.com
Questions?

Aleta Technologies provides expert support in these and other cybersecurity areas. Please contact me!

Jay Kurowsky, CISSP
President & CEO
Aleta Technologies, Inc.
256-895-8870
jay.kurowsky@aletatechnologies.com