NAVFAC Cybersecurity of Industrial Control Systems Industry Day Meeting
September 22, 2015
Martin Luther King Jr. Memorial Library

Question & Answer Notes:

CISCO

- Question: Cisco: are you planning on moving into the process control networks, detection etc. A lot of that equipment isn't network ready.

  Answer: A lot is becoming IP enabled, talking over networks. Part of the solution is identifying those devices to identify what is connecting to the device. ID medical devices running the script to enclave it and protect it from the network.

- Question: Mentioned risk management framework; we have to conform to the DISA as well. Can you talk about how we comply with all the security requirements? STIG has multiple requirements

  Answer: The framework is about what controls we have to pick – It is considered in the RMF to implement, the RMF has a whole area on implementation. NIST realizes this is a living document and we need to consider inputs from government and private sector.

MAR

*Q: None

JACOBS*

*Q: None

Contract support of OUSD AT&L (EI&E) Business Systems & Information Office handed out CDs with the "Cyber Security Evaluation Tool" Version 7.0.

DELL

- Question: Do your firewalls have capability to do ICS protocols?

  Answer: I don't know, but can get back to you. We are fully STIG comliant

IBM

- Q: None

SYMANTEC

- Question: Embedding the agent in the PLC – vendors we deal with won't let us change the embedded OS, do you work with manufacturers to allow this within the HVAC/SCADA?

  Answer: We have in limited fashion. There is a lot of movement within the medical device community. We are also working with vendors in the IOT, but not in the OT space. More proactive ICS vendors are baking security into new.

  The four zero-day attacks were windows based, STUXNET, so we stopped it on the outer perimeter. We don't embed on a controller, unless it's running something like LINUX.

PARSONS

- Q: None

SPLUNK

- Question: You mentioned analysis across different types of information you're bringing in, are those analysis, widgets, plugged into any new deployment? Or do you customize them?

  Answer: They can be customized. McKenny created a B-doc app that runs on SPLUNK that gives the data they want. As data comes in they will index them to ID key value pairs.

- Question: The Navy partners we're doing business with are interested in systems across geographic locations. For theater fuel delivery: how much of my ability to deliver fuel is assured or compromised – compared to a single data center. For a given mission, is this percentage secure?

  Answer: If that information is resonant within that database, then yes SPLUNK can review that. So, in order to measure that there needs to be a record. As long as SPLUNK can review and analyze the data it can be done.

- Question: Is there a way to look at the supporting infrastructure (delivering fuel) you are at this percentage of risk across the total aggregate "mission package" as opposed to a given data center/location?

  Answer: Yes, as long as you have a measurement of those pieces of data.

Ultra Electronics, 3eTI (Added to agenda)

- Q: None

QUESTION SUBMITTED ON NOTECARD

- Question: Will there be another round of RFI responses collected, or a venue for Industry to provide further information about ICS Cybersecurity to NAVFAC?

- Answer: There is not another Industry Day for Cybersecurity of ICS planned. Industry can use the NAVFAC email NAVFAC_Cybersecurity@navy.mil to provide information to NAVFAC to consider. Additionally, remaining questions and clarifications can be sent to the same email address. All information submitted to the email address in response to this RFI will be considered proprietary and for official government use only.