EFCOG Monthly Meeting

January 27, 2021

Announcements and Updates:

- DOE 414.1-4 Software Guide not yet in REVCOM
  - Review has been signed off by Todd Lapointe, Deputy Associate Under Secretary for Environment, Health, and Safety and is now with Matt Moury, AU-1, for a final check
  - Once Matt approves, then it will go get permission to go into REVCOM
  - Once it is in REVCOM, Christian will let Vicki know and she will let everyone know
- Possibility to have a meeting to help engage individuals that want to participate in REVCOM and provide comments
- Update on AU-32 position Christian has made a selection. An announcement will be made to this group next WebEx.
- Future of Central Registry still under Senior Management Consideration
  - HQ might not be able to support it like in the past due to shortage of the workforce
  - Possibility to make a sub-task group to help fill that roll and work with HQ to figure out how to make it easier to maintain
- Christian highly recommends and requests that everyone create and account and sign up for the QA Community of Practice on Organizational Excellence Website https://orgex.energy.gov/
  - Username is generally your email
  - Signup for the QA Community of Practice and EFCOG forums
- Talks have begun about the Spring 2021 Virtual Face-to-Face Meeting.
  - Tentative dates are April 19-22
  - They have checked with NQA-1 committees and other subcommittees to make sure that the time doesn't overlap with other events
  - Vicki will be hosting the Webex meeting
    - Please try to join the meeting via computer because it is the best way and can avoid issues rejoining the meeting

Task Group Updates & Discussion:

- **SQA-20-01: Better Application to All Software (**Pat Auer-leader)
  - The white paper has been finalized and is available on the EFCOG website
  - This paper can be found at the bottom of the website in a folder called *WHITE PAPERS*

- **Definition of Graded Approach (Lance Abbott, SRS/Jeni Turgeon, SNL, Co-leaders)**
  - Question to turn into position statement then turn into a small white paper or to end the task? How to share this information?
    - Team will take it offline and discuss
  - This task is considered closed
  - Can you grade to zero? Do we need to say it?
    - Team will take another look at that (it is all about right sizing)

- **Cloud-based Hosting Whitepaper (Russell Swannack - WHITE PAPER IN DRAFT)**
  - At any point in time people can add comment to the white paper located in BOX
  - Still waiting for comments from team
  - Since not everyone doesn't have access to BOX Vicki will send it out to the larger group

- **Software Standards and Orders (Cristy Renner, Fluor BWXT, Leader)**
    - This is located on the EFCOG website in the White Papers folder
        - This will be a living matrix as additions as they get more information
    - A new standard that has been added and the working sheet has new updates that have links that will take you to the standards
    - Vicki will take the updated version from Jan 19 and add it to the EFCOG website
    - Put together a spreadsheet and it is located on the Box site
        - Feel free to reach out to Cristy by email for input or questions
        - Utilize the main workbook and create a sheet with your name and add your document for people to populate information within the columns
        - If you can also fill out your sheet and send it to Cristy and she will compile the information.

Possible New Subtasks:

- Alternates to Central Registry Toolbox
- Coordination with Defense Programs/NEA SQA Initiative
- IoT (internet of Things) from the presentation notes are located lower
- Testing Spreadsheets
- Veronica Camarillo-Morris is willing to restart the subtask team How to Manage Configurable Devices
- Any other ideas please email Vicki

DOE O 4141E Task Group:

1) **Better Application to "All" Software**
    a) Pat Auer, LLNL, Leader
    b) Marylou Apodaca, SNL
    c) Veronica Camarillo-Morris, LANL
    d) Stella McKirdy, INL

2) **Software Standards and Orders**
    a) Cristy Renner, Fluor BWXT, Lead
    b) Annette Coonfield, WRPS, Deputy
    c) Clyde Armstrong, Tru Project
    d) Orlando Ferrer, RL
    e) Faith Girolamo, SRS
    f) Kamie Hopper, SNL
    g) Alvin McClerkin, OREM
    h) Abhijit Sengupt, HQ
    i) Dave Thoman, Amentum

3) Graded Approach for Software

a) Lance Abbott, SRS, Co-leader
b) Jeni Turgeon, SNL, Co-leader
c) Marylou Apodaca, SNL
d) Carol, Olijar, ANL

4) Cloud-based Hosting Software

a) Russell Swannack, PNNL, Lead
b) Lisa Cooper, Paducah
c) Orlando Ferrer, RL
d) Vicki Pope, LLNL

Next Steps

- If you have something you would like to present or want to share (e.g., a tool or process used at your site or another software-related topic of interest) please contact Vicki, Teri or Marylou
- Please consider joining or leading a subtask group. You can join by responding to these meeting minutes
- Don't forget to post your Task products to Box

PRESENTATION: Solar Winds Incident and IoT for Federal Networks by Greg Pope, CSQE @LLNL

The Solar Winds incident got the attention of a lot of people and they asked the question "could this happen here?"

The Solar Winds breach, which is also called the red-eye incident, was not a single attack. The company was Solar Winds and the product was Orion, which is a network management software. Orion is used by over 30,000 customers world-wide including the federal government. The attack was done to the source code by a hacker group that was able to log on to the Solar Winds software configuration management tool by overriding the Multi Factor Authentication (MFA). Initially it was like a phishing scheme that allowed them to gain a username and password and the hackers signed in that way to bypass the MFA. Then the hackers added small bits of source code over course of 3-4 days and setting a timer so that the changes wouldn't take effect until 2 weeks later.

Another customer of the Orion product, Fire Eye - a cyber security company, had their cyber security tools stolen as part of this attack. Since the attack was to the source code it was updated to the 30,000+ customers allowing the hacker group to attack between 12,000-14,000 customers. This attack or intrusion occurred in April 2020 but was not discovered until December 2020. It was discovered by accident when the person who had their username stolen realized that someone was changing their source code. The same day it was discovered, Solar Winds created and released a checker to look for the signature in the code to determine if customers had the malware. Once it is discovered that there has been a change to the binary code, tools can be made very quickly to resolve the issue.

Some things that can be done to prevent this in the future:

- Check the .Net files, which is a Component Intermediate Language (CIL) a part of the install media, and detect any changes or compare against the release notes
- Look for a timer
- Look for an IO port or URL port that is not recognized

PRESENTATION: IoT (Internet of Things) Devices by Greg Pope, CSQE @LLNL

IoT device examples that are accessible via Wi-Fi

- Ring Doorbell
- Smart home security
- Home appliances
- Wearable health devices

These devices are meant to be low cost. Adding security adds more code, which in turn reduces battery life. This begs to ask what if we wanted to connect these types of devices up to government network? The item that might be of most interest for the government to use would be sensors because they measure flows, chemical compositions or even moisture levels. There is a potential use for these devices to be put on the network and don't want it to be a new interface for an intrusion threat.

The National Institute of Standards and Technology (NIST) is writing a guidance document, "IoT Device Cybersecurity Guidance for the Federal Government" with the idea that you would need to comply with the requirements guidance before you put these devices on the network. NIST SP 800-213 (Draft) is looking for comments and will be open until Feb 12, 2021 iotsecurity@nist.gov . This document is to provide guidance to the government to help them make the technical and nontechnical requirements to put IoTs on a government network.

Sample of requirements for IoT devices:

- Shall have unique identifiers
- Have the availability to have the firmware updated for vulnerabilities
- Data at rest shall be encrypted
- No default passwords (which could be an automated checker)
- Passwords not stored in plain text (which could be an automated checker)
- Multiple privileged levels of access (admin, general user)

Ideas on how to enforce:

- Review IoT device specifications (Labor intensive)
- Audit manufacture's development (Labor intensive)
- Create tools that verify firmware compliance
- Start an EFCOG group to be proactive and look for ways of enforcing the NIST standards
    - If any interest on this subtask please reach out to Viki Pope, or Teri or Marylou

EFCOG Monthly Meeting
January 27, 2021

Attendance:

If anyone attended this meeting, but does not see their name on the list, please contact Marylou Apodaca (marapod@sandia.gov).

- Chair: Vicki Pope (pope13@llnl.gov)
- Vice Chair: Teri Vincent (teri.vincent@cns.doe.gov)
- Secretary: Marylou Apodaca (marapod@sandia.gov)

First Name	Last Name	Site
Lance	Abbot	SRS
Sid	Ailes	Atkins Global
Patrick	Auer	LLNL
Gregory	Baker	
Todd	Billings	Bechtel
Tom	Bundy	ORNL
Veronica	Camarillo-Morris	LANL
Annette	Coonfield	WRPS
Lisa	Cooper	PPPO
Mary	Curtis	FNAL
Yevonne	Deaton	DOE-EM
Orlando	Ferrer	RL
Faith	Girolamo	SRS
Sarah	Hartson	LFO
Barbara	Hill	DOE-ICP
Kamie	Hopper	SNL
James	Hylko	Four Rivers
Kinh	Le	KCNSC
Joe	Lopez	DOE-CBFO
Diana	Marquez	
Carl	Mazzola	
Alvin	McClerkin	DOE-OREM
Stella	McKirdy	INL
Carol	Olijar	ANL
Christian	Palay	DOE-HQ
Greg	Pope	LLNL
Vicki	Pope	LLNL
Cristy	Renner	Fluor BWXT
Jackie	Salazar	LANL
Kevin	Shaw	ORNL
Russell	Swannack	PNNL
Dave	Thoman	Amentum

First Name	Last Name	Site
Gladys	Udenta	NNSA
Teri Al 208-5**-**24	Vincent Zuckero	CNS SRS
270-5**-**18		
301-2**-**78		
740-6**-**12		
816-6**-**50		

Next Meeting: February 17, 2021 @ 1:00 pm PST