When Will Investments Be Made in Cybersecuring Our Infrastructure Control Systems / Operational Technology?

COC Hack = What Year?

‘For more than a year, hackers with ties to the Chinese military have been eavesdropping on U.S. Chamber of Commerce (COC) officials involved in Asia affairs.

At one point, the penetration into the COC was so complete that a Chamber thermostat was communicating with a computer in China. Another time, chamber employees were surprised to see one of their printers printing in Chinese.

"I don't think the COC has anything worth stealing, but it's part of a pattern of the Chinese stealing of everything they can, and that's worrying," Richard Clarke, former White House counter-terrorism adviser.”

Fast forward = Solar Winds, Colonial Pipeline….

Policy Requirements for Control Systems / Operational Technology Cybersecurity

- **Control systems** monitor and control devices, processes, systems and networks in varied environments - ranging from **building, logistics, manufacturing, medical** to **weapons systems**

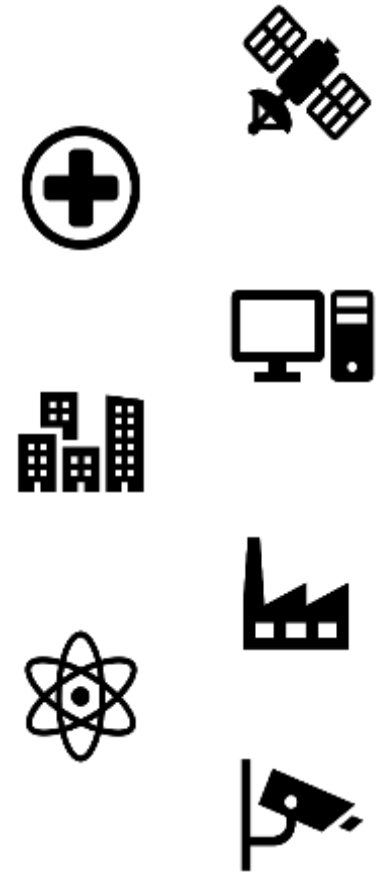
- Control systems are **subject to all cybersecurity policies**, requirements and standards for DoD Operational Technology; are 7 years into a transition to fold their cybersecurity implementation into the DoD cybersecurity program writ large (*DoDIs 8500/8510Mar'14 // 8510 update now*)

- DoD CIO is the OPR for control systems cybersecurity with a primary role to provide **oversight, policy and implementation guidance** for cybersecurity of control systems DSD Memo Jul'18

- Office of the Principal Cyber Advisor oversees / integrates DoD's control systems cybersecurity implementation via DoD Cyber Strategy LOEs DSD Memo Jul'18

- A&S has lead for cyber vulnerability assessments of Defense Critical Infrastructure NDAA FY17 S 1650

- DoD Components responsible for cybersecurity implementation and risk management of control systems for all DoD systems; **designate an OPR for their control systems** DoD CIO Memo Dec'18



E.O: IMPROVING THE NATION'S CYBERSECURITY

The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))

- **Provide recommended contract language**
- **Publish a definition of critical software**
- **Publish guidance on minimum standards for vendor testing of SW source code**
- **DHS to lead Cyber Safety review board**
- **DHS create standard playbook**
- **Maximize early detection of cybersecurity vulnerabilities & incidents**

image courtesy of cbssport.com