The Common Readiness Methodology

David Bedard, Security+, A+, CCP
Security and Compliance Analyst

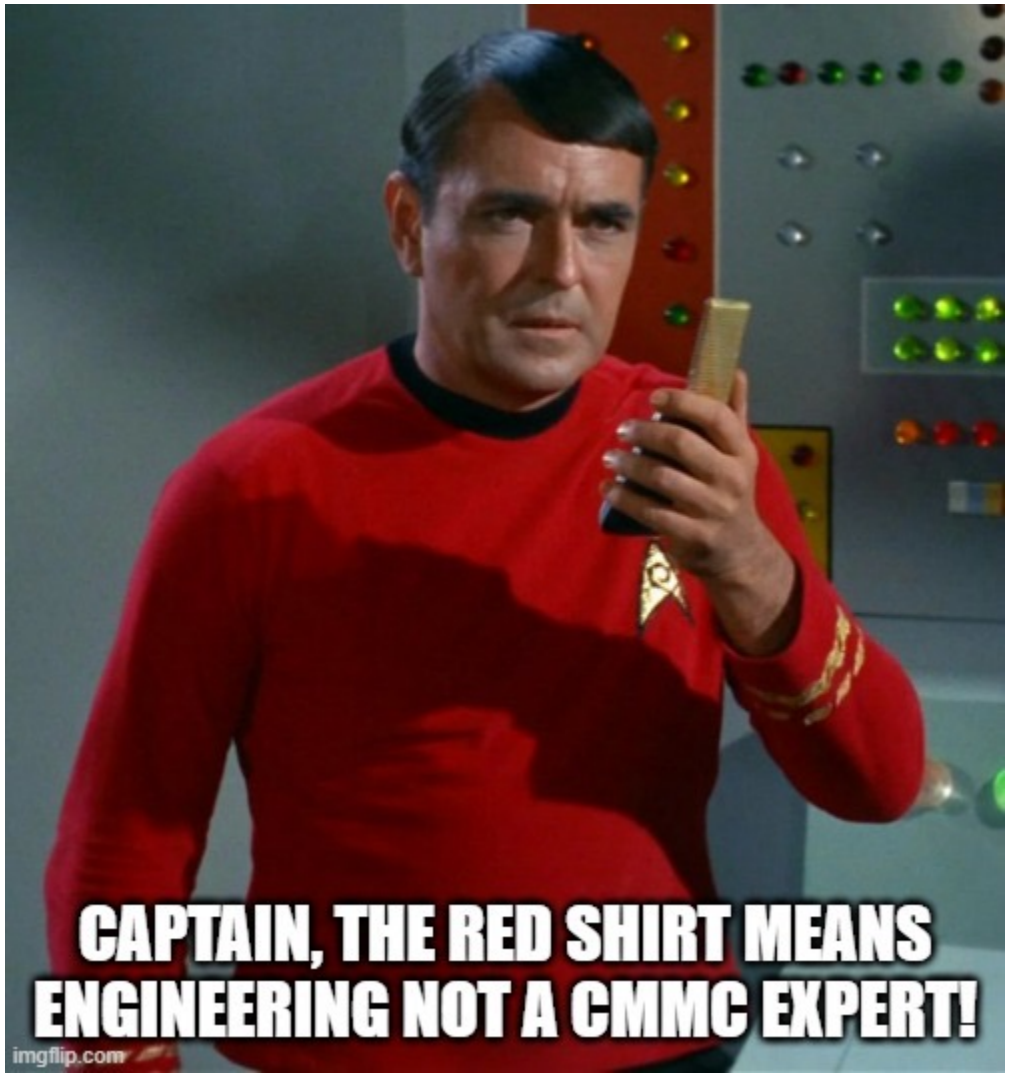
A Bit About Me

- Lead Security and Compliance Analyst
- CCP, Security+, A+
- Worked with DIB on compliance efforts in aligning with DFARS 7012 and NIST 800-171 requirements
- Assisted KTL leadership with the concept that lead to the creation and development of a secure enclave used by the 1st Authorized C3PAO

Today's Agenda

- Keep things brief
- Scoping your environment and why it's important (CMMC Level 2)
- Putting it together
- Planning
  - Gap assessment and when you should/shouldn't do one
  - Remediation
  - Certification
- DFARS 7012 Paragraph (b)(2)(ii)(D) and the FedRAMP Memorandum
- POA&M

Before We Get To Scoping



It All Begins Here

- How does FCI/CUI enter and leave your environment?

Entrances and Exits

- Answers may be:
  - Email
  - Web portals
  - DoD SAFE
  - Postal Delivery
- Did you ask the right People?

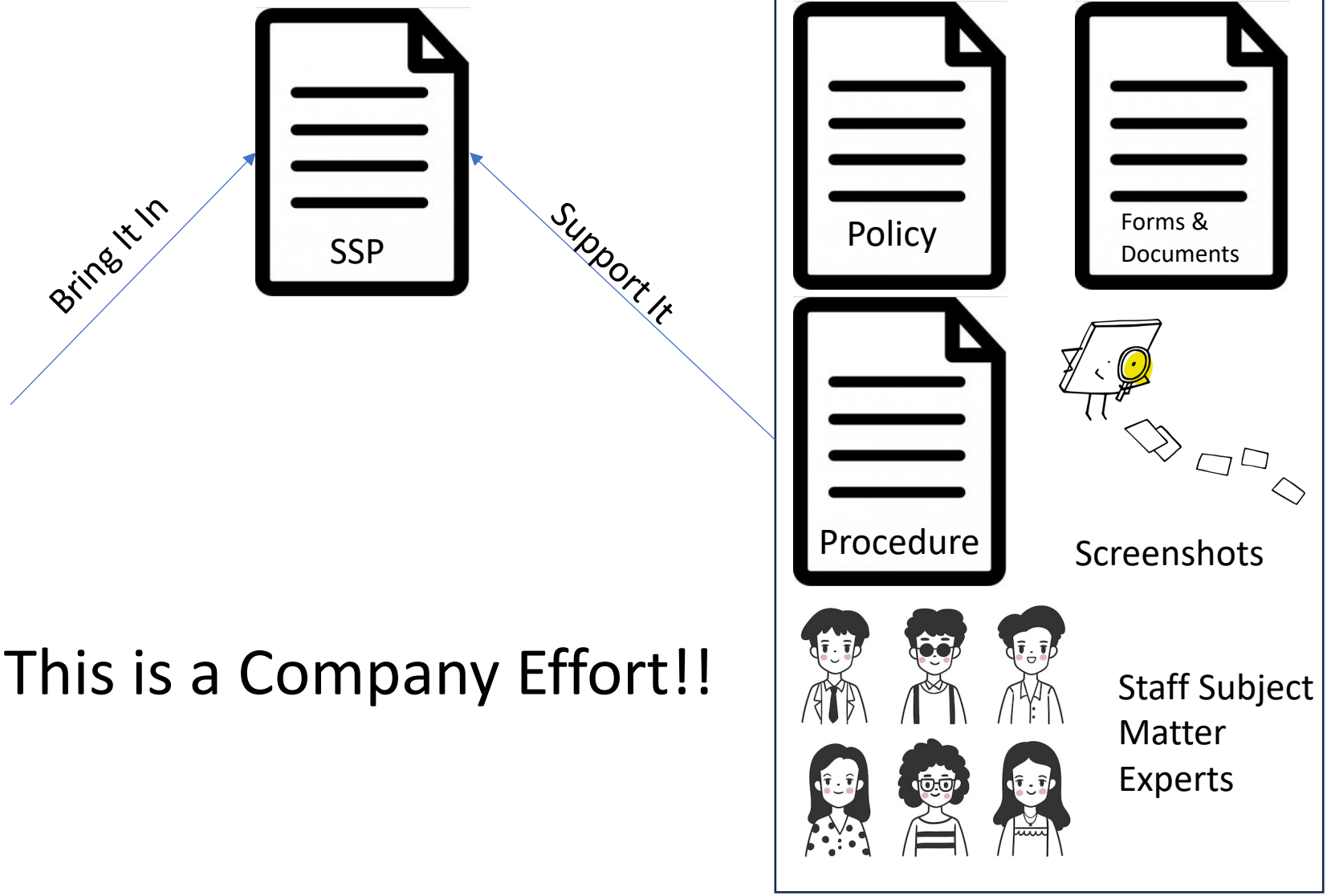
Courtesy of WikiHow

What Are Your Assets?

- **CUI Assets – Assessed against practices**
  - Process, store, or transmit CUI
- **Security Protection Assets (SPA) - Assessed against practices**
  - Provides security functions and capabilities to the OSC's assessment scope regardless of whether the asset processes, stores, or transmits CUI.
- **Contractor Risk Managed Assets (CRMA) – Not assessed against practices unless…..**
  - Assets that can process, store, or transmit CUI, but are not intended to due to policies, procedures, and practices in place.
- **Specialized Assets – Not assessed against practices**
  - Assets may or may not process, store, or transmit CUI that are a certain category (i.e. – Government property, IoT devices, Restricted Information Systems, and Test Equipment)
- **Out-of-Scope Assets**
  - Logically or physically separated assets that do not process, store, or transmit CUI
- **3 Common Criteria Except Out-Of-Scope Assets**
  - Document in an Asset Inventory
  - Document the Assets (CUI, SPA, CRMA, & SA) in the System Security Plan (SSP)
  - Include each Asset Type within your Network Diagram for the assessment scope

Putting is all together

- System Name
- System Categorization
- System Owner
- Authorizing Official
- Other Key Contacts as applicable
- System Security Officer
- Operational Status
- System Description/Purpose
- Network Diagram
- Dataflow Diagram
- Assets and Types
- Control Implementation Descriptions
- And more…



This is a Company Effort!!

What To Do

- **Gap Assessment**
  - When does it make sense?
- **Certification Preparation**
  - Spreadsheet or software solution it's up to you.
  - Remember to TIE your evidence to the assessment objective/determination statement and that it's adequate and sufficient.
    - Test your implementation of the control
    - Interview staff responsible for management of the control
    - Examine documentation, records, screenshots related to addressing the control

DFARS and the FedRAMP Memorandum

- **DFARS 252.204-7012 Paragraph (b)(2)(ii)(D)**
  - Contracted external cloud service provider used to process, store, or transmit CUI must meet the security requirements equivalent to the FedRAMP Moderate baseline.
- **FedRAMP Memorandum**
  - "To be considered FedRAMP Moderate equivalent, CSOs must achieve 100 percent compliance with the latest FedRAMP moderate security control baseline through an assessment conducted by a FedRAMP-recognized Third Party Assessment Organization…"

Clarifications Are A Must

- **FedRAMP Memorandum Clarified?**
  - David McKeown per Federal News Network Article* - “Are they good with NIST SP 800-171 or not?”
  - Call is being planned by with the industry by McKeown’s office in the next 30-45 days for more details on the memo.
- **CMMC Proposed Rule**
  - Cloud Service Provider means “an external company that provides a platform, infrastructure, applications, and/or storage services for its clients.”
  - External Service Provider CMMC Program, “CUI or Security Protection Data must be processed, stored, or transmitted on the ESP assets to be considered an ESP.”
  - Section 10 b – “OSC uses an external CSP to process, store, or transmit CUI or to provide security protection”, the CSP will provide evidence that it “meets the security requirements equivalent to FedRAMP”

* https://federalnewsnetwork.com/defense-main/2024/01/dod-aims-to-get-more-companies-through-fedramp-pipeline/

Still Time for Comments

- Monday is the last day. There's still time to comment!
  - https://www.regulations.gov/document/DOD-2023-OS-0063-0001

Careful What You POA&M

- **What to include**
  - POA&M should include tasks to be accomplished, resources required to accomplish the task, any applicable milestones, and scheduled completion dates. – NIST SP 800-37
- **POA&M Once, Affirm Twice**
- **POA&Ms for Level 2 cannot include**
  - Any control with a point value greater than 1 with the exception of SC.L2-3.13.11.
  - AC.L2–3.1.20 External Connections
  - AC.L2–3.1.22 Control Public Information
  - PE.L2–3.10.3 Escort Visitors
  - PE.L2–3.10.4 Physical Access Logs
  - PE.L2–3.10.5 Manage Physical Access
- **POA&M = Conditional Certification if score is equal or greater than 80%**
  - 180 days to close out POA&M items for Final Certification

David Bedard, Security+, A+, CCP
Security and Compliance Analyst
Info@ktlsolutions.com
https://www.ktlsolutions.com/
(301) 360-0001