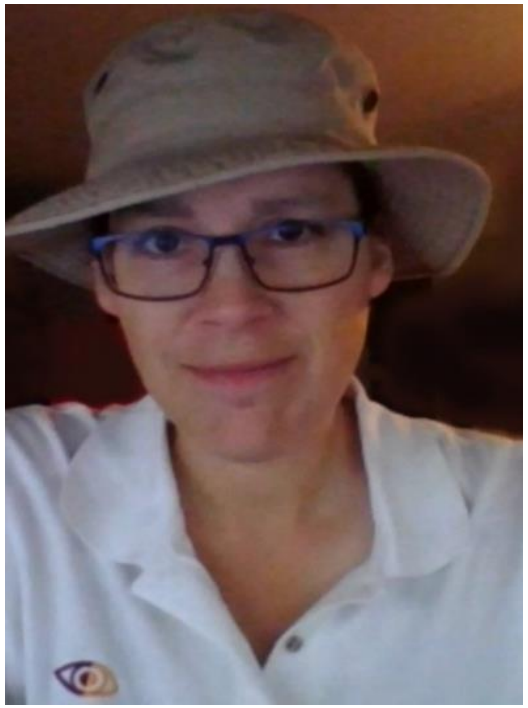
CMMC Updates
&
Building a System Security Plan (SSP)

Current As Of: July 2024

Sponsored by:

TODAY'S SPEAKERS



Amira Armond
President
Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Cassia Baker
Research Faculty
Georgia Institute of Technology

Vince Scott
CEO
Defense Cybersecurity Group
INFRAGARD DIB Sector

Sponsored by:

2 Michael

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your Contracts**
  - Your contracts should tell you what information you must protect
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Sponsored by:

Michael

CMMC Updates and Timelines

- **DoD submitted Final 32 CFR CMMC 2.0 Rule to OIRA**
  - Office of Information and Regulatory Affairs (OIRA) has 90 to 120 days to conduct review.
  - Final step in the process before public release.
  - Could see final rule published by this Fall with ~60 days before the final rule is effective.
- **48 CFR Rule to implement rule within DFARS?**
- **Timelines**
- **What does this mean?**

Vince

What is a System Security Plan (SSP)?

- **NIST Definition:**
  - A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Sponsored by:

What is a System Security Plan (SSP)?

- An SSP is crucial for CMMC compliance & not optional
- An SSP essentially describes the cybersecurity program that a defense contractor has in place to protect CUI.
- The SSP needs to go through each NIST SP 800-171 control and include how the control is implemented, monitored and enforced.
- Out in the field, we find that nearly all the SSPs that we've come across are inadequate to meet requirements.

Sponsored by:

Cassia

System Security Plan – What do I document?

- SSP: primary source of cybersecurity policies
- Identifying systems, artifacts, procedures, and plans
- Documenting can help identify shortfalls in processes
- Unsure whether to document? Document it!

Vince

Where do I start with my documentation?

- At ground zero?
  - GRC platform may help organize
  - Boiler plate templates
- Some documentation?
  - Consider independent trusted advisor
  - Beware of group think
- Almost there?
  - Congratulations!
  - Have someone check your work
  - Avoid blind spots

Vince

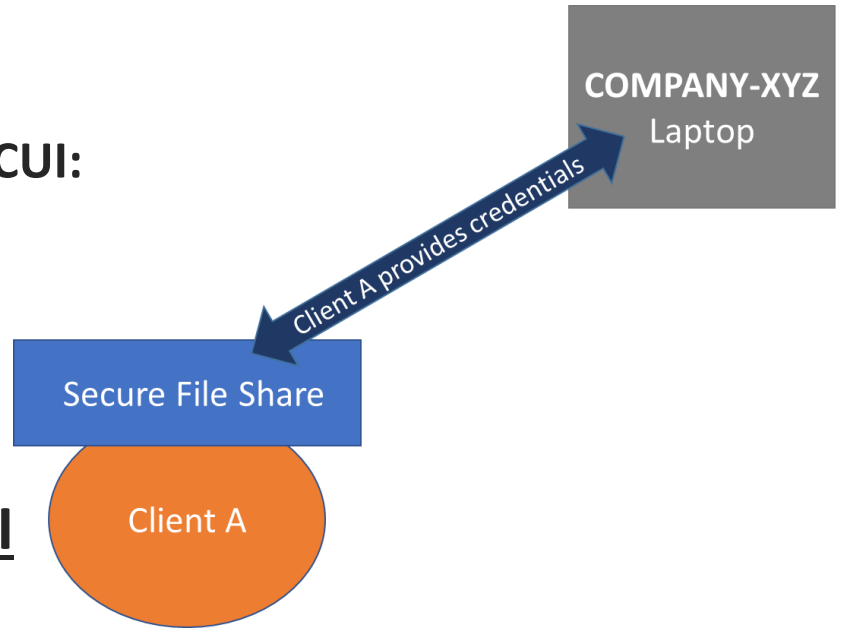
Building a System Security Plan (SSP)

- **Overview of "Section 1"**
  - **Information System Name/Title: <COMPANY-XYZ-INFORMATION-SYSTEM>**
  - **System Categorization: Moderate Impact for Confidentiality**
  - **System Unique Identifier: <COMPANY-XYZ>IS-001**
  - **Information Owner**
  - **<CIO>, <CISO>, (etc)**

<COMPANY-XYZ> may encounter the following types of CUI:

- Controlled Technical Information
- Export Controlled
- General Critical Infrastructure Information

Data Flows for CUI



Sponsored by:

Amira

Building a System Security Plan (SSP)

- **“Section 2” - introducing your system to the reader**
  - Minimum 1 paragraph per type of system. High level explanation of security (how managed, how logged, how protected, what security function it serves)
    - Laptops / phones
    - Servers / Databases
    - Clouds / external service providers
    - Firewalls, network, WIFI *network diagrams*
    - Facility, badge system, datacenter protections, *facility diagrams*
  - Should we discuss CRMAs and SAs, even if they ‘won’t be assessed’?

Sponsored by:

Amira

Per practice – SSP Section 3

System Security Plan

Explain your scope, explain your systems, explain major protective measures

Refer to Procedure?

Per practice:

- Policy/procedures that support
- Describe how implemented
  per system
- Controlling measures (to discover and fix failures)
- Schedule, trigger, or continuous
- Who performs the activity

Optional but recommended:

- Describe where to find evidence
  - Path to configuration
  - Database or list
  - Records kept at _____
- Tie answers to the Assessment Objective
- Identify exact section number in referenced docs

80%+ of SSPs from companies requesting CMMC assessment are not up to standard

Sponsored by:

Building a System Security Plan

- **Other uses of a System Security Plan**
  - "Defines" – if information or a value does not need to be known outside the IT department, it can be defined inside the SSP.
  - Identifying how requirements are inherited from other providers
  - Identifying "tests" for requirements, to verify controls are working
  - Reference other SSPs relevant to environment

- **Appendices –**
  - Firewall ruleset and explanations why ports/protocols/services allowed
  - Identify roles/responsibilities, related training requirements

Amira

Building a System Security Plan

- **More than one SSP:**
  - More than one information system in scope?
  - Lots of physical locations?
  - Dev network?
  - MSP network affects your network's security due to VPN connections?
  - Split the SSP up?
  - Why have multiple SSPs?

Amira

Building a System Security Plan

- **Should you purposefully be obtuse in your SSP?**
  - "The company performs requirement" – but no further information?
  - If you are going to be obtuse, then where do you give the real information?
  - What about publicly facing SSPs?

Sponsored by:

Amira

Questions

Sponsored by: