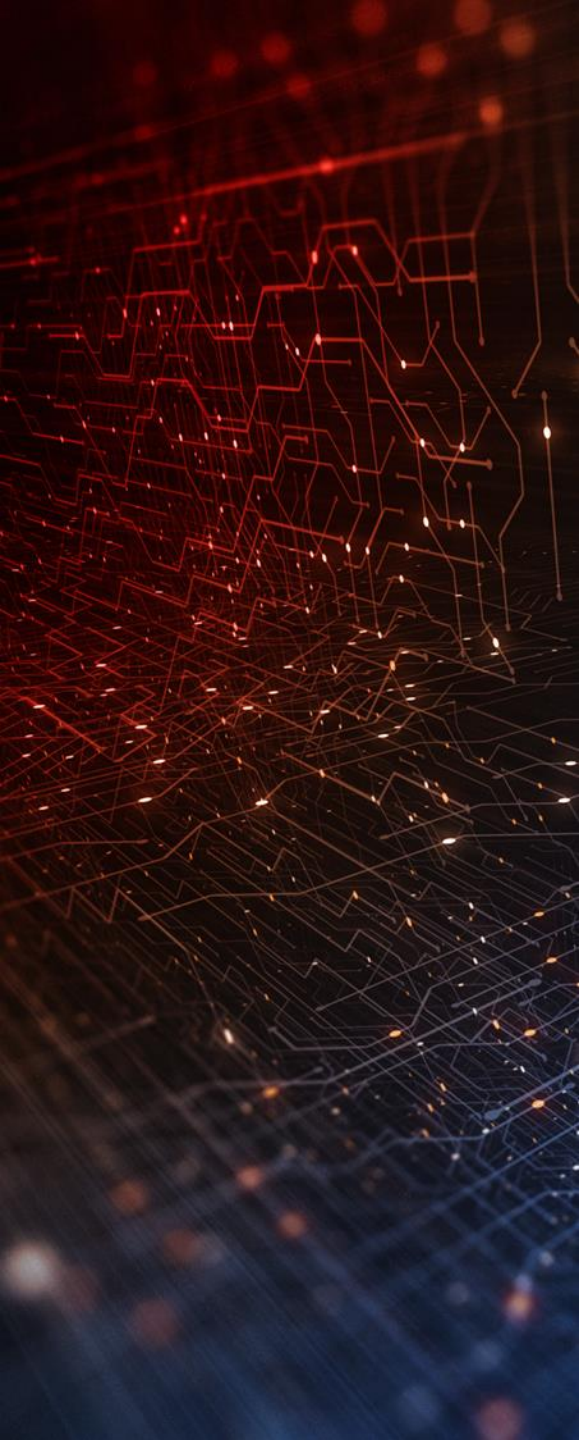
INFORMATION SYSTEM SECURITY OFFICER (ISSO) ESSENTIALS

LORA WOODWORTH

INTRODUCTION

- Over 20 years of experience in a variety of cybersecurity roles
- ISSM for 8+ years
- ISSO for 10 years
- Mainly support classified systems for the Department of Defense (DoD)



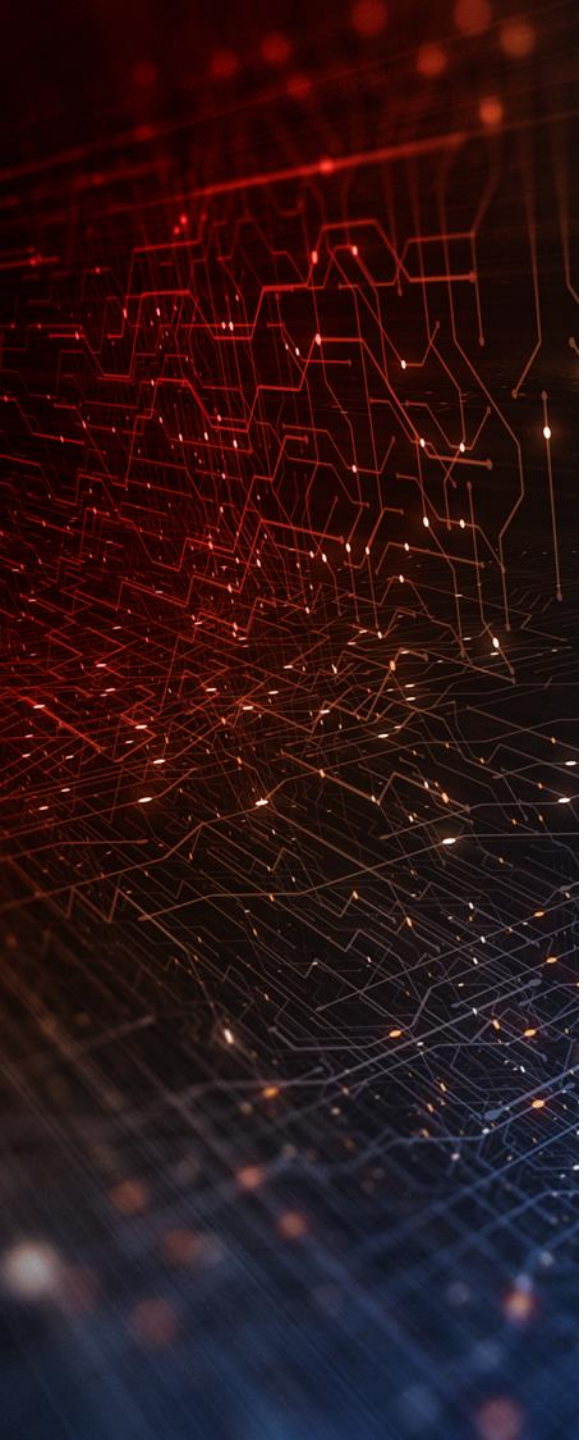
PURPOSE

Just an overview of what information is needed to maintain the security of an accredited system

There is ALWAYS MORE TO LEARN

Does not cover information needed to get an initial Approval To Operate (ATO)

Knowledge is organized using the Risk Management Framework (RMF) outlined by the NIST SP 800-53 and DCSA Assessment and Authorization Process Manual (DAAPM) ver. 2.2



ISSO RESPONSIBILITIES

- “An ISSO is an individual responsible for ensuring the appropriate operational security posture is maintained for a system. The ISSO will be assigned by the ISSM and appointed in writing. The ISSO must be an U.S. citizen and employed by the cleared contractor or its subcontractor. **The ISSO assists the ISSM in meeting their duties and responsibilities**.” DAAPM 2.2
- ISSO responsibilities vary significantly and are usually dependent upon the Organization.
- Start with the Body of Evidence (BoE) submitted to obtain an ATO
  - determine the quality and make sure it is current, identify who is responsible for maintaining it.
- How does the ISSM want to be notified of any issues, findings, vulnerabilities, or concerns that you find?
- Know your guiding documentation (i.e., DAAPM, 32 Code of Federal Regulations (CFR) Part 117 National Industrial Security Program Operating Manual (NISPOM), NIST SPs, DoD regs, ICDs, etc.)
- Complete all training as identified in the DAAPM and the system training policy

SETTING THE STAGE

This briefing was created as a tool to guide discussions and a learning path for someone learning about the different aspects of an accredited system

If you can clearly answer each question, you can say you know your system and you should be able to easily maintain it’s accreditation

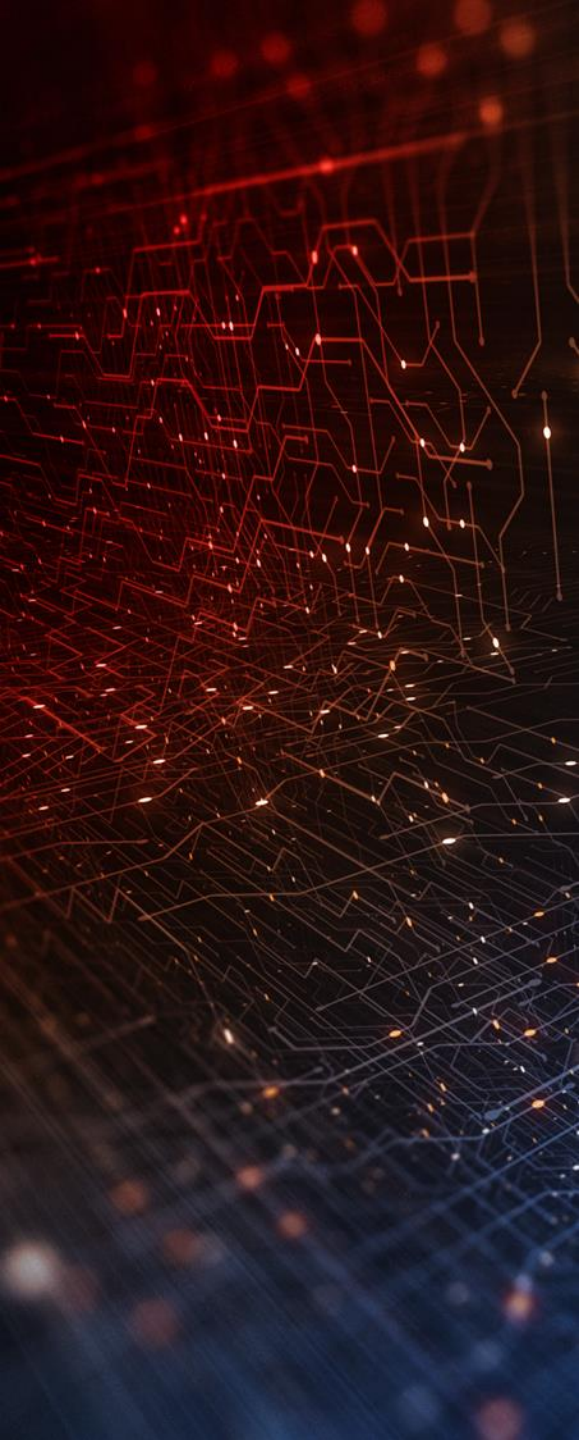
Should be applicable to ISSO’s assigned to a single system or be able to scale to much more complex networks

New people are a fresh set of eyes and might see things that the rest of the team has become blind to, don’t be afraid to ask questions or point out things that don’t seem clear

CONFIGURATION MANAGEMENT (CM)

Getting to know your System

- Review the Hardware and Software lists of the system
  - Know where everything is physically/logically located
  - How and Who maintains these lists?
  - Identify any End Of Life (EOL) issues
    - Review Hardware Warranties and support contracts, who keeps track of this information
    - Research all software vendor EOL notifications
  - Review and know the Change Management Process
    - What activities require prior approval?
    - Who is involved in the approval process?
    - What is the procedure to use?
    - Is there a formal Configuration Control Board (CCB) ? Who are the members
    - What are the ISSO's roles and responsibilities within this process?



AUDIT AND ACCOUNTABILITY (AU)

- What is being audited on the systems?
- Which components have Audit Logs and where are they stored?
- Who performs the Audit and when is it performed?
- What is an Indicator of Compromise (IoC) for this system?
- What is done with findings? Who is responsible?
- What alerting/notifications are available/implemented?
- What is normal/noise on the system?

SYSTEM INTEGRITY (SI)

PATCH MANAGEMENT

Who is responsible for Patch Management?

What is the lifecycle of a patch?

- How is it tested?
- When is it installed
- What are the thresholds that must be met?

VULNERABILITY MANAGEMENT

Where and how are vulnerabilities identified?

What are the metrics that must be tracked for a vulnerability?

What are the reporting requirements?

How does the Patch Management process support the Vulnerability Management activities?

ACCESS CONTROL (AC) AND IDENTIFICATION & AUTHENTICATION (IA)

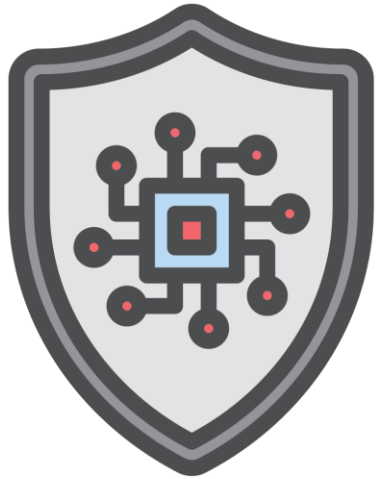
- Identify the Account Management process (Account Creation, Maintenance, deletion, modification)
- User Types - are there multiple? Who tracks? How are they assigned?
- Does the architecture or processes protect and isolate the data?
- Privileged Users – How are they identified? Who are they? And what privileges do they have? Is the number limited and who selects them?
- What is the device and service identification and authentication process? Is it automated or manual?
- Does your system use Multifactor Authentication (MFA) or Hard Tokens? Who maintains or issues these items?
- Do users get multiple accounts for different roles? How are they trained to use the different accounts? How is it enforced?

RISK ASSESSMENT (RA)

- Review the System Risk Assessment Report (RAR) it should contain:
  - Threats and vulnerabilities to the system
  - The Open-Source Software (OSS) on the system and the mitigations that are in place to minimize the risk
  - The perceived risk to running the system
- Has your organization and Information Owner (IO) determined their Risk Tolerance? Do they match or are they out of sync with one another?
- What is the process to pull in Vulnerability and Scanning information? How is it incorporated into the RAR?
- Is the RAR a part of an organizational or higher-level Risk Management Process?

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

- Network Diagrams – Does it match what you know of the system? Who maintains them and when do they get updated?
- Identify your accreditation boundary and ensure it is enforced
- Know where your data is and where it goes.
- Identify all other services and protections (DNS, Cryptographic protections, Mobile Code, Malicious Code protections, separations, etc.)
- Determine any other required protections
    - Legal, executive order, regulations, corporate policy, system policy, best practices, guidance from industry partners



INCIDENT RESPONSE (IR) AND CONTINGENCY PLANNING (CP)

Determine where your Incident Response and Contingency Plans are.

Ensure the Notification Procedures are up to date.

Determine who plans/schedules tests for the plans and when the last time the plans were tested.

Ensure you know how to backup and restore the system if it goes down.

AWARENESS AND TRAINING (AT)

- Identify what training is needed for the different types of users
- Go through all the training and ensure you understand everything in it.
- Determine when the refresher training is given and how
- Identify how status is tracked and reported
- Verify all users have received the appropriate training and that it is current

ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)

- How is your system assessed?
- Where is the Body of Evidence (BoE) maintained, who is responsible for keeping everything current?
- Who performs the necessary activities to maintain the ATO?
- How is the system monitored to ensure it maintains compliance?
- What is the Continuous Monitoring Strategy?

MAINTENANCE (MA)

- How is the system maintained?
- Who performs the maintenance?
  - If a 3rd party or vendor maintenance is needed, what are the procedures for that?
- How is it reported/monitored?
- What metrics are tracked to show that the system is properly maintained?
- Are there any routine maintenance activities that the ISSO needs to track, perform or schedule?

MEDIA PROTECTION (MP)

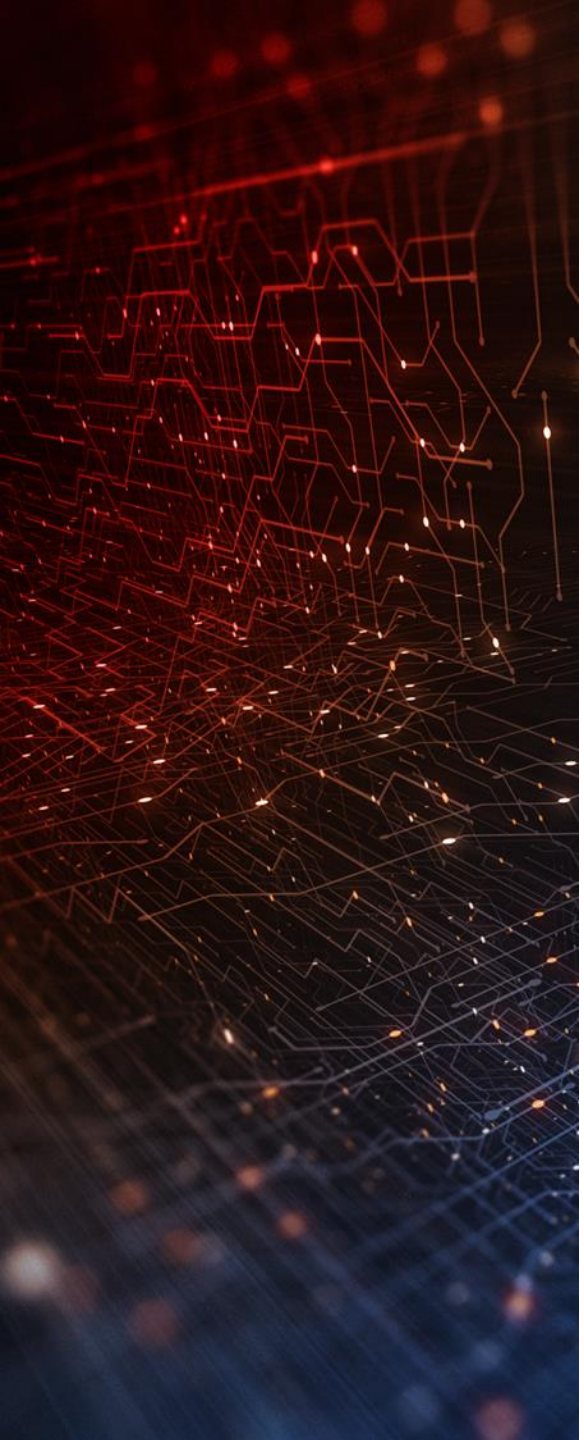
- What media is allowed on the system?
- Who can bring data into the system?
- What are the procedures/guidelines for bringing media into the system?
- What if any media can be used to take data off the system?
- Who is authorized to take data off the system?
- Where can it go? (High to High only, or is High to Low transfers authorized) Can it leave the building?
- How is the media protected before and after it is used on the system?
- How is the media marked?
- Are there Cover sheets or Labels already available?

SYSTEM & SERVICE ACQUISITION (SA) AND SUPPLY CHAIN RISK MANAGEMENT (SR)

- What software is allowed on the system?
- How can a user get new software on the system?
- Are there development activities allowed on the system?
- What is the System Development Life Cycle and what is done to ensure proper safeguards for the system/data?
- Who ensures the Supply Chain is Secure?
- How is a Security Analysis performed for new software and the Supply Chain?
- What is the ISSO role in the Acquisition and Supply Chain process?

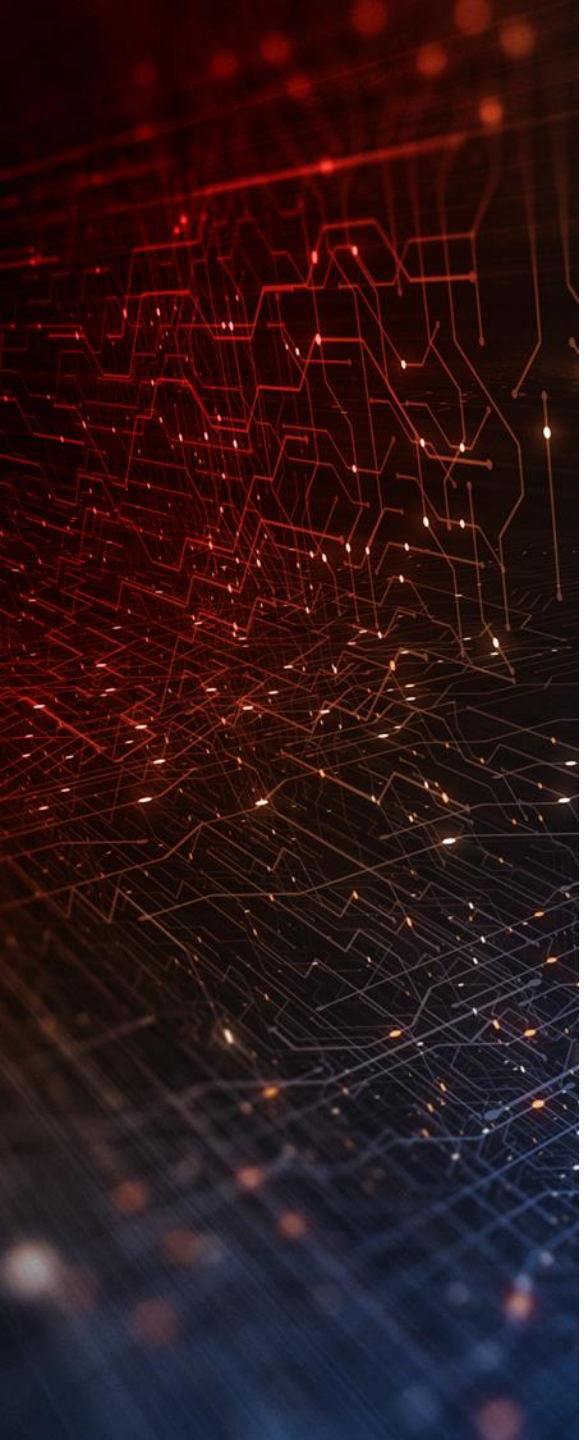
PLANNING (PL) AND PROGRAM MANAGEMENT (PM)

- Read the Information Security Program Plan for the System
  - Is it clear and does it match the system as you have learned about it?
    - Identify the Measures of Performance – verify all metrics are being tracked and reported in accordance with the plan
  - Review the Plan of Action and Milestones (POA&M)
    - Identify current activities and deadlines for those activities
    - Know the process and who manages the POA&M entries
  - Review the Mission and Business functions and Concept of Operations
  - Determine the Disclosure alert process and identify who is responsible
  - Identify Leadership Roles and ensure they are all accurate
  - Review the documented Security and Privacy Architectures and make sure the system matches what is documented



PHYSICAL ENVIRONMENT PROTECTION (PE)

- Determine who is responsible for Physical security (Facility Security Officer (FSO), Office Manager, Facility Manager, Building Security, etc.)
- Review the facility with the person in charge of the protections
  - Identify emergency protections (Lighting, power, water, fire, etc.)
  - Determine how visitors are given access to the area
  - Review who is allowed access to the area and how those rules are enforced
  - Determine the role that an ISSO needs to play in the physical security of the system



PERSONNEL SECURITY (PS)

- How are employees screened?
- What is the on-boarding process and how is the ISSO and the system involved?
- What is the termination process and how is the ISSO notified/by whom?
- How are transfers handled and who notifies the ISSO if system access is no longer needed?
- What is the insider threat process?
- What are the sanction levels and how is that enforced?

APPLICATION

- These questions can be used to develop a training briefing for ISSOs with the answers outlined for their specific system
- Used by the ISSM to identify gaps in their security program
- Portioned out to other teams as necessary (system administration, facility management teams, vulnerability management, etc.) as a training program

QUESTIONS?

- Lora Woodworth
  - LinkedIn: www.linkedin.com/in/lora-woodworth
  - NCMS Hub