Simulators Program Office *Cybersecurity Review*

Demica Ware Robinson

AFLCMC/WNSE

Demica.robinson@us.af.mil

7 May 19

Cleared for Public Release 25 Apr 19 (88ABW-2019-2020)

Disclaimer: The information provided herein represents the Government’s best understanding of the procurement as of the presentation date. This information should be considered preliminary and subject to change.

Cybersecurity Initiative

- The Simulators Program Office leads the development, acquisition and sustainment effort necessary to meet the MAJCOMs simulation and training requirements
  - WNS currently has 30+ cyber specialists working the transition to the Risk Management Framework (RMF)
  - New Cybersecurity paradigm – RMF – all systems are required to be Assessed and/or Authorized for use
    - Many existing contracts have been modified to support RMF
      - Requires fully certified staff (ISSOs and ISSMs) to meet the requirements per DoDD 8570.01M

ntsa
Ohio Chapter

Risk Management Framework

SIMULATORS
CONCURRENT AFFORDABLE TRAINING

Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and PAO&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

•We need cybersecurity support to fully understand this process!

Current Challenges Answering Controls

- Answering Security Controls as identified in NIST 800-53 rev4
  - WNS ISSMs face challenges with prime contractors providing quality artifacts to support compliance/non-compliance
    - ISSMs spend considerable amount of time “training” prime contractor’s cybersecurity personnel on the proper way to answer controls
    - Documentation is often sent back and forth multiple times before final acceptance by the program office

Current Challenges Answering Controls

- Collateral systems are required to submit all Authority To Operate (ATO) documentation via the Enterprise Mission Assurance Support Service (eMASS) database on SIPRNet (DoDI 8510.01)
  - Many of the prime contractors do not have access to SIPRNet
  - Requires document delivery via secure mail

Current Challenges Vulnerability Scanning

- Performing vulnerability scans as required by the Authorizing Official (AO)
  - Collateral systems are required to use the Assured Compliance Assessment Solution (ACAS) vulnerability scanning tool
  - WNS has deployed and trained personnel on site to perform vulnerability scans – requires personnel to keep software updated and licenses up to date (documentation is left onsite and “reach back” to the Program Office is available)

Issues/Concerns

- Different requirements to obtain an ATO among the different AOs
  - Must understand the unique requirements to each AO
  - WNS currently works with 5 different AOs for authorizations
- Cybersecurity Support Contractors:
  - Challenge is keeping qualified candidates (DoDD 8570.01M). High turnover due to high demand for qualified cybersecurity workforce
  - Problems with continuity supporting the programs

DoD Approved 8570 Certifications

DoD Approved Baseline Certifications		
IAT Level I	**IAT Level II**	**IAT Level III**
A+ CE CCNA-Security Network+ CE SSCP	CCNA-Security GICSP GSEC Security+ CE SSCP	CASP CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH GCIA GCIH GICSP SCYBER	CEH GICSP SSCP	CEH GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CISA GSNA	CISM CISSP-ISSMP	

Takeaways

- Cybersecurity staff must understand and comply with (at a minimum)

DoDI 8500	DoDI 8510
NIST 800-53 rev 4	AFI 17-101

- All cybersecurity support personnel must be certified in compliance with DoDD 8570.01M
  - ISSOs must be certified at least to IAM Level I
  - ISSMs must be certified at least to IAM Level II
- Cybersecurity personnel must understand how to answer security controls necessary for obtaining authorization and provide proper artifacts to support those answers

SIMULATORS

CONCURRENT AFFORDABLE TRAINING

Questions?