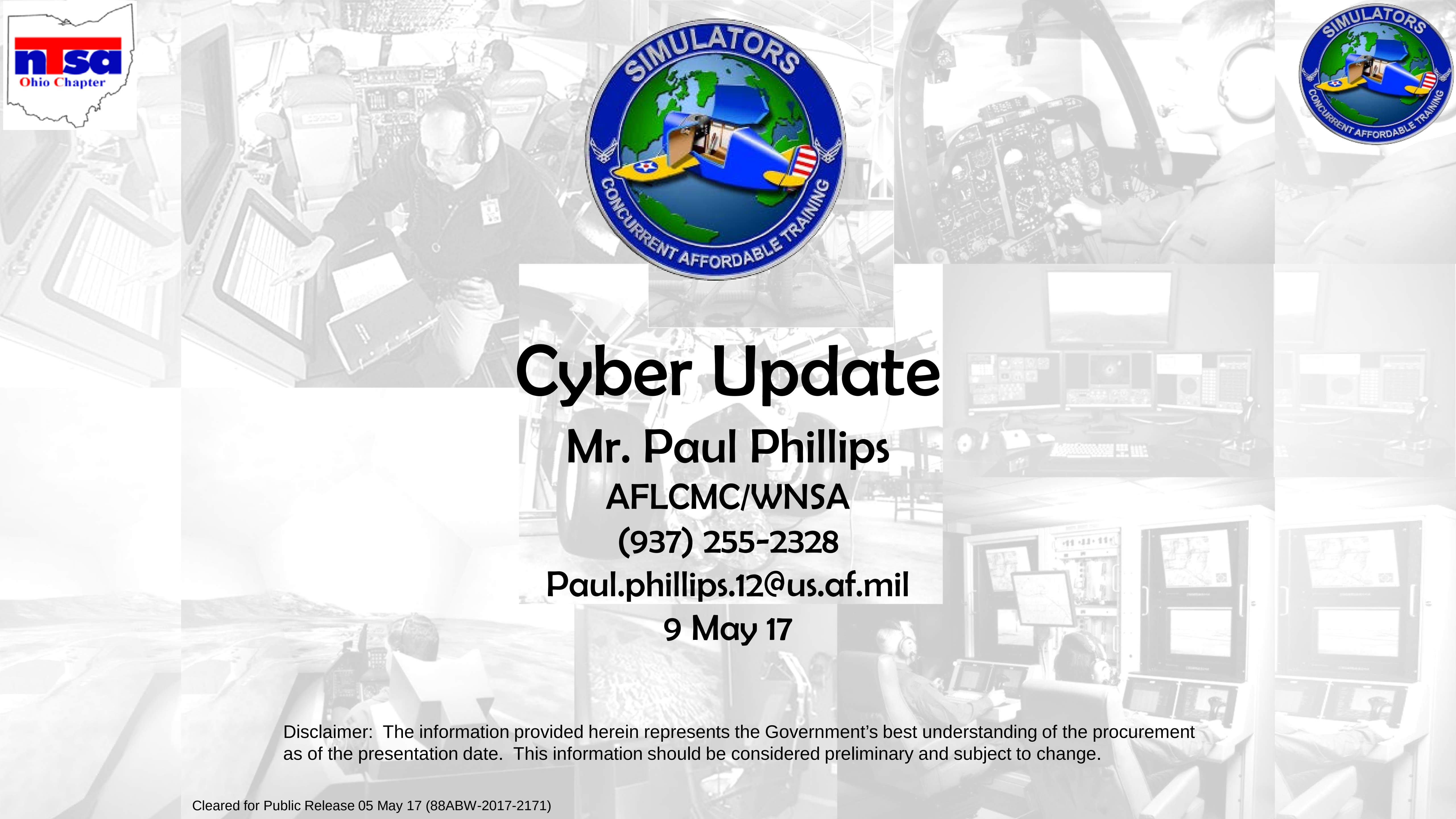


Cyber Update

Mr. Paul Phillips

AFLCMC/WNSA

(937) 255-2328

Paul.phillips.12@us.af.mil

9 May 17

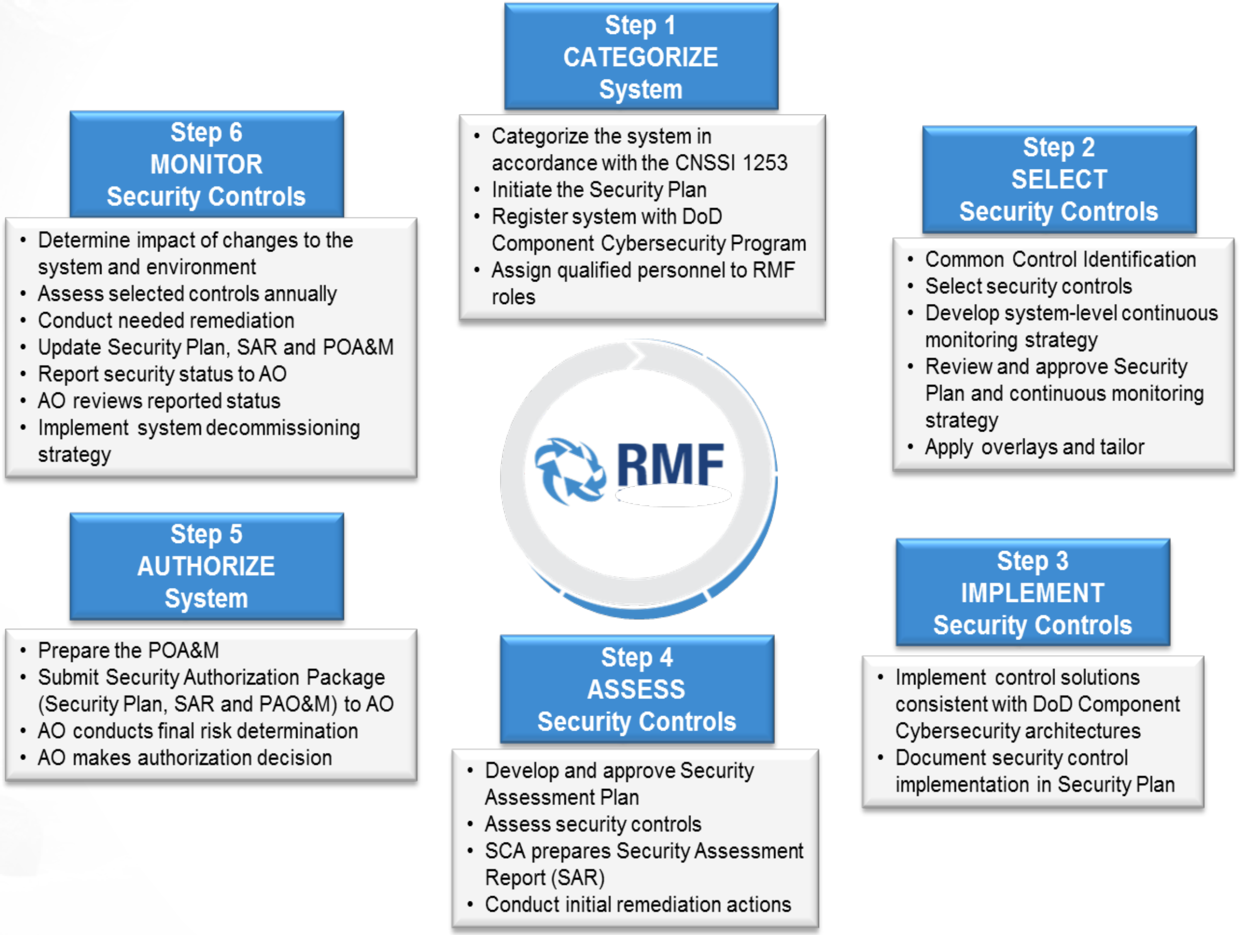
Disclaimer: The information provided herein represents the Government's best understanding of the procurement as of the presentation date. This information should be considered preliminary and subject to change.

Cleared for Public Release 05 May 17 (88ABW-2017-2171)

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 systems are legacy and pose challenges to update
    - Many existing contracts have been modified to support RMF
      - Requires additional time and money
      - Requires fully certified staff (ISSOs and ISSMs) to meet the requirements per DoDD 8570.01M

Risk Management Framework



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 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
- Performing vulnerability scans as required by the AO
  - Collateral systems are required to use the Assured Compliance Assessment Solution (ACAS) vulnerability scanning tool
  - Special Access Programs may use other vulnerability scanning tools in addition to ACAS

Current Challenges

- Collateral systems are required to submit all 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
- Special Access Programs are required to submit all ATO documentation via the Air Force SAP Assessment and Authorization Tool (AFSAAT) – per SAF/AAZ memo (01 Feb 2016) deployment has been delayed
  - Many of the prime contractors submit documentation via secure download

Issues/Concerns

- Many systems use unsupported operating systems
  - Transition to Windows10
  - Secure Host Baseline (SHB) – preferred
    - If use of SHB is technically not feasible, documentation is necessary to request a waiver from the Authorizing Official (AO)
- Different requirements to obtain an ATO among the different AOs
- 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 rev4
  - DoDD 8570.01M
- 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?