HOW SYSTEMS SECURITY ENGINEERING (SSE) ADDRESSES CYBERSEUCRITY-RISK MANAGEMENT FRAMEWORK (CYBER-RMF) FOR TEST & EVALUATION (T&E) PROJECT MANAGEMENT

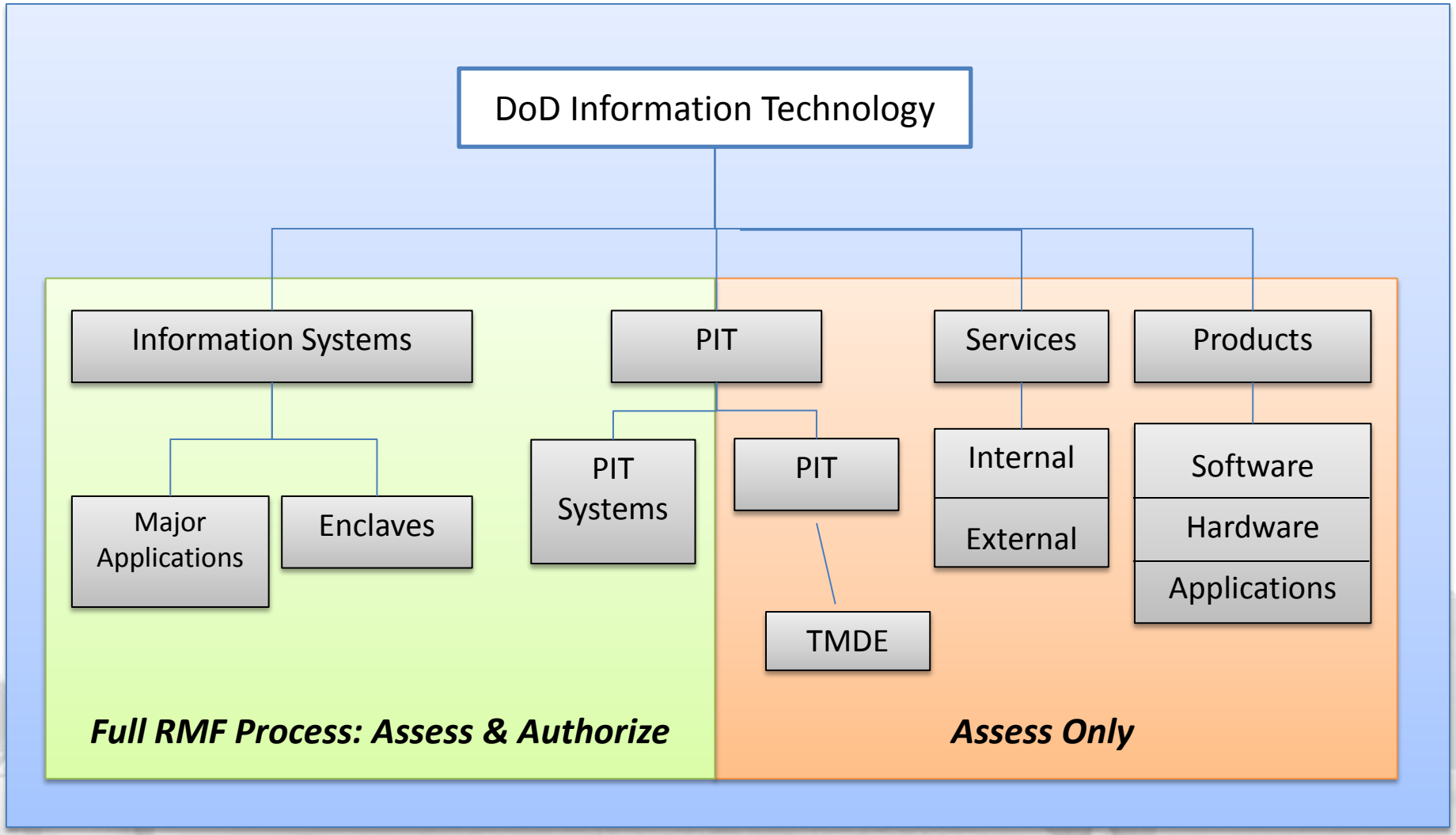
Presenter

Harry Cooper II
JT3 LLC, Corporate
RMF-Cybersecurity Lead

Join the collective that is the new RMF-Cyber…resistance is futile.

This is why…we must stay vigilant.

Cybersecurity Protection of IT within T&E Program Management



What exactly is Cybersecurity? (Cyber)

Prevention of damage to, *protection* of, and *restoration* of computers, electronic communications systems, electronic communications services, wire/wireless communication, and electronic communication, including information contained therein, to ensure its *availability*, *integrity*, *authentication*, *confidentiality*, and *nonrepudiation*.

DoDI 8500.01, Cybersecurity/CNSSI No. 4009, CNSS Glossary

What is Risk Management Framework? (RMF)

- A structured approach used to oversee and *manage risk* for an enterprise.

Test Range Cyber-Focus Areas

- Systems Security Engineering (SSE); a subset of Systems Engineering (SE), addresses stakeholder security requirements & concerns within projects/programs throughout it's life-cycle.
- Cybersecurity (Cyber) is applicable to Test Range Environments (Policy Mandate!)
- Risk Management Framework-Cybersecurity (RMF-Cyber) applicable to Platform IT within T&E

Systems Security Engineering (SSE) Process

Systems Security Engineering (SSE) - Integrates research, development and technology protection into the Systems Engineering Process.

Goals: prevents or delays exploitation of information & systems that host the information.

SSE Applicable RMF-Cyber Artifacts

- ✓ Modeling schemes, complex code, scripts, etc.
- ✓Documented configuration settings/test plans,
- ✓Documented security tasks/procedures

Security (built-In) instead of …(bolted-on) after-the-fact

T&E (Range) Environment IT Project Management

- Project/Program/Task Leads Must:
  - assign Cybersecurity Representative to the Team
  - address Cybersecurity for all IT at the beginning of the project (Requirements/Definition Phases)
  - address RMF (Risk Management Framework) for all IT
  - receive approval-to-operate for all Information Technology before use

Cybersecurity Support Personnel

- ISSM/ISSO

(Info-Systems Security Manager/Officer)

- ISSE

(Info-Systems Security Engineer)

- ISSA

(Info-Systems Security Analyst)

- ISSS

(Info-Systems Security Specialist)

RMF-Cybersecurity Approval Chain

- AO-Authorizing Official
- SCA-Security Control Assessor
- SCAR (R-Representative)
  - eMASS Package Submission
- ISO (Info-Systems Owner)
- Program/Project/Task (Manager/Lead)

  * ISSM/ISSO

  (Info-Systems Security Manager/Officer)

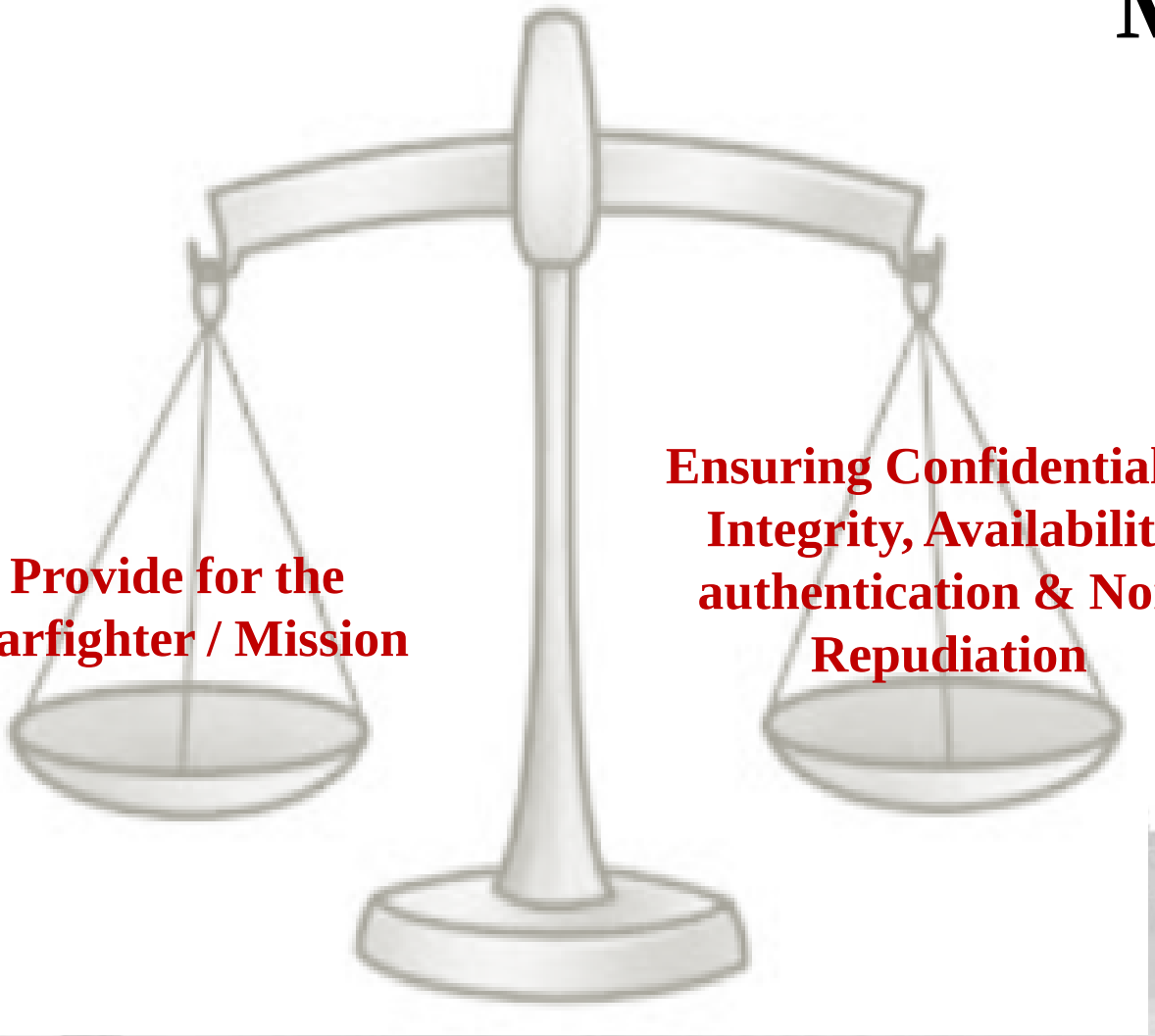
  * User Representative (UR)

Goal: Acceptable Level of RISK

Mission Risk

vs.

Cyber-Risk



Provide for the Warfighter / Mission

Ensuring Confidentiality, Integrity, Availability, authentication & Non-Repudiation

Question & Answer Session ?

(Initial) Cybersecurity Package: Categorization of the System/Asset

- CIE – Cybersecurity Impact Evaluation with/CONOPS
- System/IT Asset Topology Diagram
- Cybersecurity Assessment document/report (Artifacts/Initial SITG Scans results, etc.)
- Hardware List
- Software List
- Firmware List

RMF (Artifacts)
Security Authorization Package
(Assess & Authorize)

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POA&M)
- Authorization Decision Document (Signed Memo); ATO, IATT, DATO etc.)
- Risk Assessment Report (RAR) and all specifically required supporting artifacts, documents, diagrams, STIG/ACAS scan results, etc.