# TRMC Cybersecurity Status


8 MAR 2018

Robin Deiulio

TRMC Cybersecurity

# Agenda

- TRMC Cybersecurity Capability
- Current Cybersecurity Projects
- TRMC Software Certifications
- TRMC Applications utilizing Software Assurance Process (TENA Tools)
- Current Cybersecurity Issues
- RDT&E Overlay
- TRMC Websites Services (TWS) Cybersecurity

# TRMC Cybersecurity Capability

- The TRMC is establishing a cybersecurity capability as part of the TRMC support role to RDT&E under the DoD 8510.01, Risk Management Framework (RMF). The TRMC is ultimately responsible for TRMC systems.

**TRMC Current Systems**

- **JSN System Control Center (SYSCON)**
- **JSN SYSCON Active Measurement Program (JAMP)**
- **TRMC Website Services (TWS)**
- **Multi-Level Secure Joint Coalition Network Environment (MLS-JCNE) (2 enclaves)**

# Current Cybersecurity Projects

- **TRMC Cybersecurity** – Overarching Policies in development
  - **Assess & Authorize Process for systems**
  - **eMASS considerations**
  - **In-House Software Certification Assessments (TENA Tools)**

- **Continuous Monitoring** – Current Systems
  - **JAMP (Darin Crowley, ISSM)**
  - **JSN SYSCON (Darin Crowley, ISSM)**
  - **TWS (Robin Deiulio, ISSM)**
  - **MLS JCNE UNCLASSIFIED ENCLAVE (Robin Deiulio, ISSM)**
  - **MLS JCNE CLASSIFIED ENCLAVE (Robin Deiulio, ISSM)**

# Current Cybersecurity Projects (Cont.)

| TENA SOFTWARE APPROVALS | |
|---|---|
| Air Force E/APL | Renewal |
| Army CoN | Renewal |
| Navy DADMS | 6/27/2011 |

| TENA SOFTWARE Certifications | |
|---|---|
| TENA Console | In progress |
| TidV | In progress |

## Joint RDT&E Reciprocity Overlay Team (JRROT)

The RCC-CSG has agreed to champion the RDT&E Overlay as the FMCO. TRMC the main POC for the RDT&E Overlay for improving reciprocity, and identifying recurring RDT&E constraints to accompany an ATO to manage risks

## Defense Research and Engineering Network (DREN)

TENA protocol and TENA-based applications approved for both DREN and Secret DREN (SDREN)

## Unified Cross Domain Services Management Office (UCDSMO)

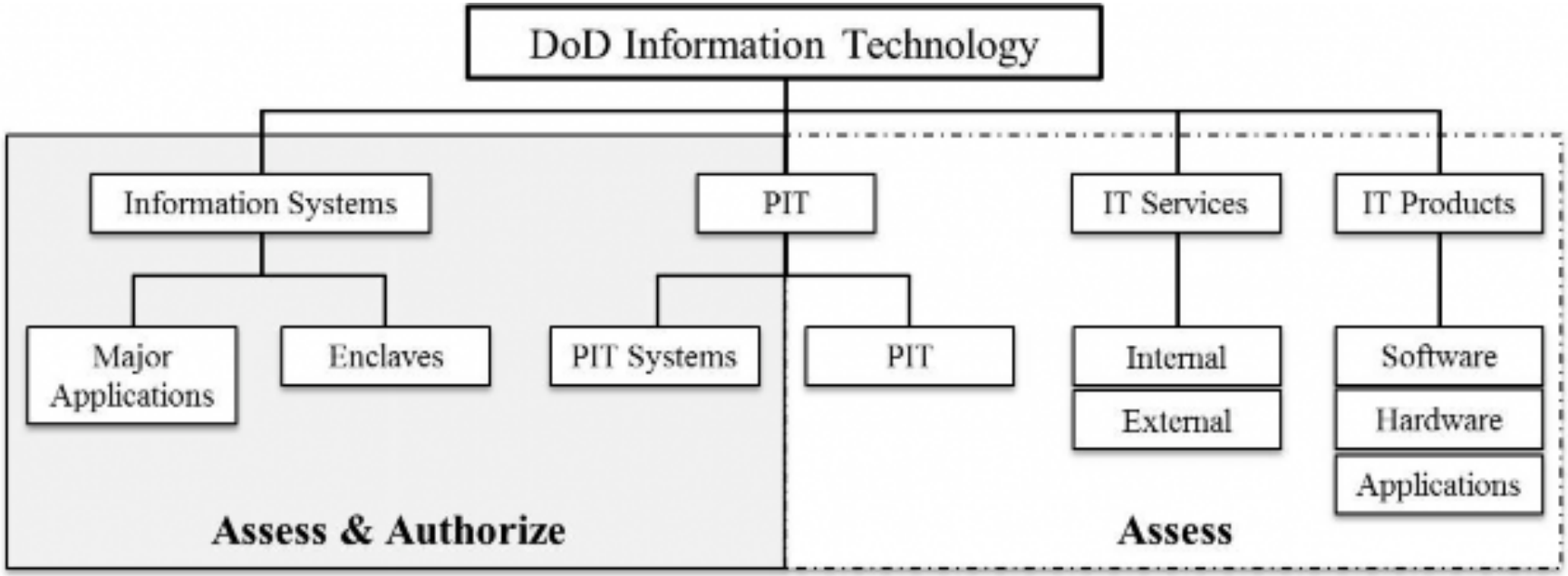
TENA-enabled Cross Domain trusted guard SimShield v3 on baseline list

## Non-Classified Internet Protocol Router Network (NIPRNet)

Eglin JTTOCC (including TENA Middleware) obtained an ATO on NIPRNet

# TRMC Software Certifications

- Applications configured IAW applicable Security Technical Implementation Guides (STIGs), Security hardening procedures, Best Business Practices, under an ISSM and SISO




DOD 8510.01 Image 1

# TRMC Applications (TENA Tools) utilizing Software Assurance Process

- TRMC Web Services (TWS)
- TENA Repository
- TENA Build System
- TENA Middleware
- TENA Installer
- TENA Execution Manager
- TENA Console
- TENA Canary
- TENA Gateways
- TENA Adapters
- TENA Multicast ClearPath
- TENA Multicast Sniffer
- TENA Video Distribution System (TVDS)
- TENA Protocol Dissector (TPD)
- Interface Verification Tool (IVT)
- SIMDIS & SIMDIS TENA Plug-In
- TENA Data Collection and Playback System (TDCS)
- JMETC LiveDisk
- TENA Native Interfaces
- MLS-JCNE Applications

# Current Cybersecurity Issues

- Software Assurance and Approval Mechanisms
  - **Separate agency approval methods**
  - **Lengthy timelines for approvals**

- RMF Assess & Authorize (A&A) Procedures
  - **Processes for Implementation are different, confusing, or do not exist**
  - **Resources to hire Cybersecurity professionals are sparse**

- Misc. Requirements & Technical Issues
  - **Third Party Validators**
  - **HBSS**
  - **Continuous Monitoring**
  - **Cyber Campaign Requirements**

# RDT&E Overlay

**Overlay** - *A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the "RMF Selection" that is intended to complement (and further refine) security control baselines. Overlay specifications may be more stringent or less stringent than original security control baseline specifications, and are applied to multiple information systems.*

- Address cybersecurity concerns for 3 broad areas**:**
  - **Data Type** confidentiality and integrity risks (e.g., SCI/SAP, classified, privacy, CUI/export-control)
  - **System Functionality Needs** (e.g., CDS, space systems, tactical systems, industrial control systems and critical infrastructure )
  - **Environmental Types** (e.g., RDT&E sites/ranges, IO ranges and training sites/ranges)
- Approval bodies:
  - **Committee of National Security Systems (CNSS)** (e.g., Space Platform, Cross Domain Solution, Intelligence, Classified Information, and Privacy)
  - **National Institute of Standards and Technology (NIST)** (e.g., Industrial Control Systems)
  - **Department of Defense (DoD)** to be posted on **RMF Knowledge Service**

***The DoD RDT&E community operates in an unique environment that can SIGNIFICANTLY benefit in utilizing an Overlay to determine security controls appropriately apply an Information System***

# Why an RDT&E Overlay is Needed

- Refine, improve, and document joint cyber security policy to minimize adverse impact to missions
- Utilize reciprocity with the reuse of cyber security risk assessments
- Assist in the determination, when and under what conditions it is customary to accept risk in controlled RDT&E environments not generally tolerable in operational environment
- A common RDT&E overlay will provide tenant PMs with a common set of hosting environment control practices and RMF controls that tenants may or must inherit from within their respective hosting environments

# Joining forces in support of RDT&E

- We recognize input and partnership between TRMC, the RDT&E COI and RCC-CSG (formerly RCC-DSG) is essential to continue successful input for the RMF TAG in support of the RDT&E community.

- Previously TRMC presented the RDT&E Overlay to the RCC-DSG to accept as a RMF framework, however they did not have the authority to continue with the effort. Now that the CSG has been created, the RCC-CSG is interested in utilizing the framework of the RDT&E Overlay to support the CSG Cybersecurity reciprocity goals.


11

# Current Agency Comparison Status

*JRROT*
*Miriam Britt*

*Army RDT&E*
*BBP*
*Tristan Gilbert*

*Air Force Turbo*
*ATO Process*
*Dr. Waters*

*Navy RDT&E*
*RMF Guidance*
*John Mueller*

**16 Unique Controls**

**17 Unique Controls**

**55 Unique Controls**


U.S. AIR FORCE


*Reciprocity?*

*Duration?*

*What Organization produced the Documentation?*

*AO Status*

*Cross Domain Solutions?*

*Zone Definitions Compatibility?*



12

# Beyond the Overlay

- Create Joint RDT&E RMF Authorization Process
  - Efficiency
  - Simplicity
- Create System Guidance for RDT&E common architecture
- Create Categories of systems/enclaves
- Create Plug In Templates

# Where do we go from here

- Submit Comparison of RDT&E Services Implementations to the RCC-CSG
- Form a TRMC and Joint Service Team (with RCC representation) to work on an updated RDT&E Overlay
  - TRMC lead Telecoms/agendas/action items
  - Progress towards an end result
  - Create further efficiencies in the RMF process for the RDT&E community
  - Assist with greater issues dealing with RDT&E systems going through authorization.

# RDT&E Overlay Conclusion

- RDT&E overlay work is ongoing with the current comparison of Agency RDT&E implementations.

- Identified RMF policy gaps have been addressed through communication to Risk Management Framework (RMF) Technical Advisory Group (TAG) members
  - RDT&E COI suggested solutions to the RMF policy gaps are being provided to the appropriate policy members as new policy is being developed

- Input and participation from the RCC-CSG in the RDT&E COI essential

- RCC-CSG championing the RDT&E Overlay as the FMCO is critical to support Cybersecurity reciprocity goals

***RDT&E COI IS PROVIDING INPUT AS RMF POLICY IS BEING DEVELOPED***

# TRMC Website Services (TWS) - Cybersecurity

- TRMC is developing a Cybersecurity Capability for supporting the RDT&E Community
- TWS Cybersecurity Services webpage is being implemented
  - https://www.trmc.osd.mil/display/Cybersecurity
- An associate Helpdesk (JIRA) will be available to create support tickets
- Cybersecurity IPT Monthly Meetings
- Cybersecurity Lessons Learned
- Cybersecurity Best Practices


16

# Upcoming TRMC Cybersecurity Projects

Cybersecurity Requirements

RMF Processes

Software Assurance

Security IPT Wiki

Overarching Policies

Technical Issues

How can TRMC Cybersecurity help your team?

# Questions / Recommendations

Questions?