412th Test Wing

War-Winning Capabilities … On Time, On Cost

RCC-CSG PPD Committee Update

15 May 2019

Todd Jacob
812 AITS/ENIE

Approved for public release; distribution is unlimited.
412TW-PA-19245

Overview

- RCC-CSG
  - Inception
  - CSG Charter
  - CSG Focus and Functions
  - PPD Committee
- Optimizing the Administration of Cybersecurity
- Impacting the ATO Process
- Efforts To Date
- Software Assessments
- Future Efforts

RCC-CSG Inception

- Initiated: Blue ribbon committee in the spring of 2017 at the Data Sciences Group (DSG) Data Protection Committee (DPC)
- Driver: Cybersecurity is a growing topic that deserves more attention
- Activity: The CSG has held seven meetings to-date and has 50 members with representation from the 19 Major Range Test Facility Base (MRTFB)

https://www.wsmr.army.mil/RCCsite/OrgStruct/StandingGroups/Pages/CSG.aspx

CSG Charter

- Addresses, supports, and guides the cybersecurity of the test and evaluation community in support of its mission
- Identifies common challenges, processes, and solutions to foster collaborative efforts which encourage standardization and re-use of appropriate solutions
- Comprised of key technical and cybersecurity individuals from test and support organizations who seek to reduce the overall cyber risk of our test infrastructure

CSG Focus & Functions

- Key Focus Areas
  - identify and recommend cybersecurity resources for T&E infrastructure
  - provide guidance to test organizations
  - establish a forum for idea exchange
  - recommend security engineering best practices
  - influence cybersecurity policy and processes

- Key Functional Responsibilities
  - **improving the test range accreditation process** and product submissions
  - standardizing **inter-range reciprocity**
  - regularly **reviewing the cyber threat environment**
  - sharing best practices

Policies, Procedures and Documentation Committee

- PPD Membership
  - 19 members representing 12 ranges
  - Janae Roberts and Todd Jacob are Co-Chairs
- PPD Committee
  - Works to align standards, recommendations, examples, and reference documents aimed at **improving cybersecurity** and **optimizing the administration of cybersecurity** at member ranges
  - **Influences approving officials** from all services to converge on a common approach to accrediting common types of range systems
  - Focuses on compliance, design, process, resources, and training involved with obtaining and implementing **cybersecurity accreditation for range systems**
  - Identifies and documents common **architectural patterns and implementation practices** that improve the cybersecurity of range systems

Optimizing Administration of Cybersecurity

- RMF and Authority To Operate (ATO) Accreditation

  The DoD uses the NIST Risk Management Framework (RMF) to improve cybersecurity of systems. Steps include:

  – Prepare, Categorization, Select Controls, Implementation, Assess, Authorization (ATO), and Monitoring

  The Accreditation Process requires documentation:

  – System Security Plans (SSP), Configuration Management Plans, System Administration Policies, POA&M…

- Share Freely – Steal What You Can

  – Share configuration management plans, software evaluation methods, policy documents, system boundary designs…

Impacting the ATO Process

- Interact with Approving Officials (AO) and Security Control Assessors (SCA)
  - Understand how ranges can improve accreditation packages to ease the approval process
  - Foster common approaches to reciprocity agreements between AO
  - Bring range-specific issues to the AO attention
- Work with TRMC on the creation of an RDT&E Overlay
  - A common set of controls can help with reciprocity
  - Would want range specific overlays (RDT&E is too large)

Efforts To Date

- Identified High Impact Problems
  - Software Assessment
  - Applying Cybersecurity Controls to Configuration Management
  - Process Comparison Between Services/Ranges
  - Common Documents

- Lexicon
  - Document Cybersecurity terms used by different ranges
  - Army CON, CSI-N, PAO, Zone-B, P2P…

Software Assessments

- Recommendations on Software Assessments
  - Methods of Evaluation (AFNIC, Scan-Install-Scan, Install on Hardened System…)
  - Risk Assessment Rubrics
  - Software Assessment Methods (CM process)
  - Catalog of Software Evaluation Lists
  - List of tested software

Impact	Mission Impact	Data Breach	or	System Performance	or	Delay
1	Fully mission capable	No Data Compromised		System Performance not impacted		
2	Mission capable	Unclassified		System performance marginally impacted, minimal analysis required to understand impact		Same day flights, ~$XXX additional costs
3	Partially mission capable	FOUO		Loss of non-mission critical functionality, days of analysis required to understand impact		One day delay, ~$XK additional costs
4	Limited mission capability	FOUO/New Technology		Loss of mission critical functionality		3 or 5 day delay, ~$XXK additional costs
5	Non-mission capable	Classified data		Total loss of instrumentation functionality		Delay of greater than 5 days, ~$XXXK additional costs
5+	Severe	Undetected classified data exfiltration		Any impact to production system functionality		Major delay to fleet test activities, ~$XM additional costs

Attack Cost/ Level of Effort				Attack Success Likelihood: Rarely works / Low	Attack Success Likelihood: Sometimes works / Medium	Attack Success Likelihood: Always works / High
				Occasionally works		Always works
Nearly anyone can build: Nascent – Limited threat	Low cost to develop	Exists today	Easy to develop	3 Example: Network DoS		5 Example: Flash implant delivered via website/email
Criminal level organization can build: Moderate threat	Medium cost to develop	Many can develop				
Nation state organization can build: Advanced threat	High cost to develop	Few can develop	Hard to develop	1 Example: RF inject of malware into sensor or radio		3 Example: Supply chain implant in HW or firmware

Example Rubrics

Future Efforts

- CSG-PPD Software Assessment Guide
  - Targeting June 2020
  - Contact CSG-PPD if you have more immediate need
- Publish recommendations on cybersecurity requirements regarding Configuration Management
- Get Involved
  - Contact your Range Technical Representative to identify your local CSG member

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
06/05/2019	Briefing slides	14 May 2019

4. TITLE AND SUBTITLE
RCC-CSG Policies, Procedures and Documentation Committee Update

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Todd Jacob

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
812th AITS
195 E Popson Ave
Edwards AFB CA 93524

8. PERFORMING ORGANIZATION REPORT NUMBER
412TW-PA-19245

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
412th Test Wing
195 E Popson Ave
Edwards AFB CA 93524

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release A: distribution is unlimited.

13. SUPPLEMENTARY NOTES
ITEA, 14-16 May 2019. Las Vegas NV

14. ABSTRACT
The USAF requires a cybersecurity Risk Management Framework (RMF) accreditation package to be approved by Authorizing Official (AO) to grant an Authority To Operate (ATO) for all instrumentation systems installed on USAF platforms. Vendors can help the USAF obtain an ATO by delivering software and hardware that implements best cybersecurity practices such as delivering software with reduced attack surface, secure delivery of software binaries, and secure methods for installing/validating firmware. Hardware designs can assist the accreditation processes by defining non-volatile memory (NVM) characteristics and reduce the operational issues by isolating NVM. Adding options for logging control-plane and data-plane network traffic is very helpful as instrumentation systems expand the use of connected networks.

15. SUBJECT TERMS
RCC-CSG

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					412 TENG/EN (Tech Pubs)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	None	12	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified	Unclassified	Unclassified			661-277-8615