412th Test Wing

War-Winning Capabilities … On Time, On Cost

U.S. AIR FORCE

RCC-CSG PPD Committee Update

15 May 2019

Todd Jacob
812 AITS/ENIE

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

412TW

- 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

412TW

- 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 too 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 to large)

Efforts To Date

412TW

- 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

412TW

- 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