Range Commander's Council (RCC) Cyber Security Group (CSG)

Paul Waters
412 TENG Tech Director
Donald.waters.3@us.af.mil

Overview

- Objective
  - Describe Cyber Security Group purpose, activities, and longer term goals
- Outline
  - RCC Direction
    - Charter, Mission Statement
  - CSG Activities
  - CSG Future Directions
- BLUF
  - RCC is taking action to better prepare the DoD Ranges for the evolving Cyber Security environment

What is the Range Commander's Council?

- Gathering of Ranges from across DoD and NASA
  - Air Force
  - Army
  - Navy
  - NASA
- Organizational Structure Consists of:
  - Range Commanders
  - Executive Committee
    - Tech Reps
  - Secretariat
  - Standing Groups
    - Data Sciences Group (DSG)
    - Electronic Trajectory Measurements Group (ETMG)
    - Frequency Management Group (FMG)
    - Meteorology Group (MG)
    - Range Operations Group (ROG)
    - Telecommunications and Timing Group (TTG)
    - Telemetry Group (TG)
    - Underwater Systems Group (USG)
    - Sustainability and Environmental Group (SEG)
    - Cyber Security Group (CSG)

RCC Mission & Vision

- Mission
  - The RCC is dedicated to serving the technical and operational needs of U.S. test, training, and operational ranges.
  - The RCC provides a framework wherein:
    - Common needs are identified and common solutions are sought
    - Technical standards are established and disseminated
    - Joint procurement opportunities are explored
    - Technical and equipment exchanges are facilitated
    - Advanced concepts and technical innovations and potential applications are identified

Stand Up of CSG

- 17 Feb 2017 – Directed by Range Commanders to look into IA issues across all Ranges
- 26 Apr 2017 – Conducted a Blue Ribbon Panel (BRP) to discuss need for CSG
  - Potential Charter, Mission Statement, Membership and a path forward
- 22 Jun 2017 – 2nd BRP Meeting
  - Finalize CSG planning
- 18-19 Jun 2017 – Approved by RCC Tech Reps
- 19-20 Jul 2017 – Approved by Executive Committee
- CSG Meetings
  - 19-20 October 2017
  - 8-9 Jan 2018
  - 24-25 Apr 2018, Vandenberg AFB

CSG Charter

- The Cybersecurity Group (CSG) addresses, supports, and guides the cybersecurity of the Test & Evaluation community in support of its mission. The CSG identifies common challenges, processes, and solutions to foster collaborative efforts which encourage standardization and re-use of appropriate solutions. The CSG is comprised of key technical and cybersecurity individuals from test and support organizations who seek to reduce the overall cyber risk of our test infrastructure. The CSG's key focus areas are to 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, and influence cybersecurity policy and processes. Key functional responsibilities are improving the test range accreditation process and product submissions, standardizing inter-range reciprocity, sharing of best practices, and regularly reviewing cyber threat environment. Other tasks/functions will be added as necessary.

CSG Mission

- "Address, support, and guide the cybersecurity of the RDT&E 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."
  - Guidance to Vendors
  - Guidance to Test Organizations
    - Secure design elements
    - Templates for SSP wording
    - Support for cybersecurity workforce (dedicated IA staff)
    - Build culture in from beginning
    - Tools (e.g., vulnerability assessment software)
    - Resources (people, contracts)
    - Tri-service products & integration (Army, Navy, Air Force)
    - Continuity with range personnel moves across all ranges
  - Forum for Idea Exchange
  - Influencing Policy Makers
    - Standardized processes across services
    - Integrate IA personnel into the T&E process, knowledgeable about T&E rather than just admin/business
    - Need T&E seat at RMF Technical Advisory Group (TAG)
    - Reciprocity (but at what level), inter-range MOA/MOU/ISA
    - Streamline accreditation process for RDT&E

CSG Leadership

- Chair – Tony Rubino
  - 412 RANS Squadron Director, Edwards AFB, CA
- Vice Chair – Tristan Gilbert
  - ATEC-WSMR Range Operations-Real Time, WSMR, NM
- Secretary – John Mueller
  - NAWCWD Command ISSM - RDT&E, Pt Mugu NAS, CA

CSG Initial Tasks

1. RMF ATO process streamline tri-service reciprocity
2. Standardized MOU/MOA/ISA process
3. Guidance to vendors to get systems approved
4. Conduct regularly updated Threat Briefings & Create SIPR Email group
5. Create Tri-Service Idea exchange, such as a wiki

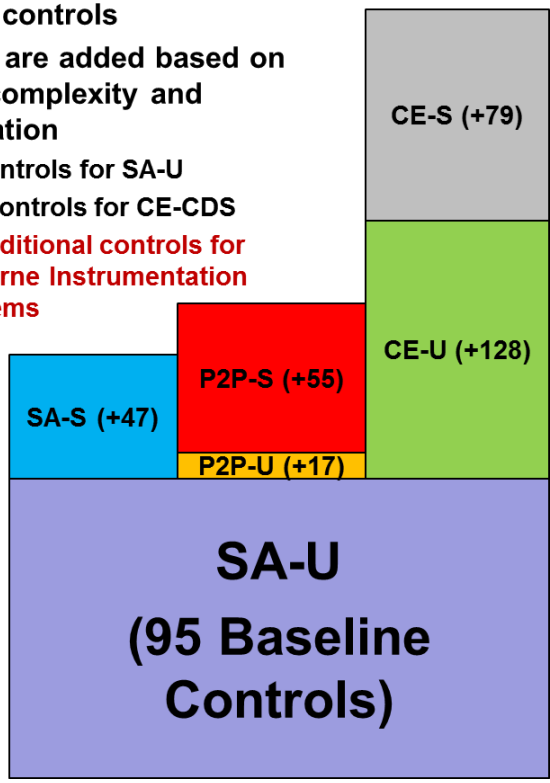
- Other Tasks:
  - Formalized two-way workflow for influencing policy makers
  - Provide cybersecurity guidance to other RCC groups
  - Cybersecurity resources and workforce development in RDT&E across all services
  - Best practices
    - Integrating realistic threat environment with cybersecurity practices
    - Integration with larger cybersecurity and cyber defense between the services

Task Status: ATO Streamline

- AFMC has a streamlined process based on typical DT&E systems
  - Sharing this process with other services and ranges
- NAWCWD has a streamlined process in coordination with the NAWCWD Security Controls Assessor (SCA)
  - Draft documentation is being shared
- Army – No tailoring identified
- Future:
  - Small working group investigating the possibility of a RDT&E Overlay
  - Looking at reciprocity processes and requirements

DT&E Tailoring

- All systems answer 95 DT&E baseline controls
- Controls are added based on system complexity and classification
  - 95 controls for SA-U
  - 388 controls for CE-CDS
  - 88 additional controls for Airborne Instrumentation Systems



Task Status: MOA/MOU/ISA

- Reviewed Range processes for interconnectivity
  - Processes and terminologies are inconsistent across ranges
  - Investigated DoD definitions and roles and responsibilities
    - Tailoring those definitions to improve interconnectivity across ranges
- Working to establish relationship between SCAs to improve reciprocity
  - Common terminology and shared concerns about controls

Memorandum of Agreement (MOA);
Memorandum of Understanding (MOU);
Interagency Service Agreement (ISA)

Task Status: Guidance to Vendors

- Air Force Test Center (AFTC) Draft Policy
  - Required for all Test Infrastructure Components use to execute flight and ground test, collect / analyze / evaluate test data, and report results
    - Acquire, Upgrade, Maintain
  - Updated DD Form 254 for security
  - Validated certificate of volatility/non-volatility
    - Identify and characterize all non-volatile storage
    - Provide supporting documentation
  - Establish Risk Management Board to manage acquisition and sustainment risks
- Future Work
  - Establish a committee to look at improved guidance in contracts

Task Status: Threat Briefings

- Threat Briefings at both CSG meetings
  - From Communications Field
  - From Intelligence Community
  - From Range Users
- Developing a SIPRNet Email Group
- Future:
  - Ongoing Local Threat Briefings
  - Proposed Top Secret Threat Briefing

Task Status: Idea Exchange

- Developing a SharePoint site to share ideas, templates, policies and other documents
  - Access through RCC website
  - https://wsdmext.wsmr.army.mil/site/rccpri/CSG/default.aspx
    - Requires RCC sponsorship for access

- Goal:
  - Be able to share answers for controls
  - RMF documents
  - MOUs, etc.
  - Processes, Local Policies
  - Potentially share threat information

Task Status: Influence Policy

- Goal is to Impact the Cyber Security Policies for DoD ranges
  - Invited SCAs from the different Range areas
    - Interaction between SCAs and Ranges
    - Interaction between SCAs with different portfolios
  - Future:
    - Invite Authorizing Officials to higher level discussion with RCC Commanders
    - Invite Policy Makers from AF, Army, Navy CIO offices

Summary

- RCC Cyber Security Group (CSG) is working to:
  - Improve security of Ranges
  - Improve authorization and accreditation results
    - Processes, documentation, reciprocity
  - Improve guidance to vendors

- Future Products
  - Cyber Security Standards for Range Systems
    - Potential process checklists
    - System Security Plan (SSP) templates and sample responses
    - Common interconnectivity agreements - reciprocity
    - Tool requirements for monitoring, data diodes, and cross domain solutions

QUESTIONS