318th Cyberspace Operations Group
Real-Time Ops & Innovation

Col Steven J Anderson
Commander

The Overall Classification Of This Brief Is
UNCLASSIFIED

Real-time Operations & Innovation (RTOI)

BY ORDER OF THE COMMANDER
AIR FORCE SPACE COMMAND

AIR FORCE SPACE COMMAND
INSTRUCTION 10-170

1 JULY 2015

Operations

CYBERSPACE REAL TIME OPERATIONS AND INNOVATION (RTOI)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at http://www.e-Publishing.af.mil for downloading or ordering

RELEASABILITY: There are no releaseability restrictions on this publication

OPR: AFSPC/A2/3/6W

Certified by: HQ AFSPC/A2/3/6W (Mr. Sidney P. Pollok)

Supersedes: AFSPCGM2013-10-01, 26 November 2013

Pages: 17

This instruction implements portions of Air Force Policy Directive (AFPD) 10-17, *Cyberspace Operations*, and provides Commander, AFSPC (AFSPC/CC) guidance for conducting RTOI activities. This instruction applies to HQ AFSPC, Twenty-Fourth Air Force (24 AF), assigned AFSPC wings, aligned Air Reserve Component (ARC) units, and all other assigned AFSPC operational and sustainment forces. All AFSPC/24 AF units shall comply with this AFSPCI, except when statutory requirements, Department of Defense (DoD)/Joint Staff or DoD Financial Management Regulations (FMRs) direct otherwise. Air Force Life Cycle Management Center (AFLCMC) may use this AFSPCI in advising HQ AFSPC and 24 AF on whether proposed projects should be designated as RTOI, and (by agreement) providing transition and sustainment resources for designated multiple-use RTOI projects before or after Capability Release for Operational Use. It also applies to all military, government service, and applicable contractor personnel whose duties directly relate to the management, operations, maintenance, mission assurance, preparation, and conduct of activities required in support of AFSPC cyberspace missions. This instruction shall be updated every two years, or more frequently as needed to reflect the most current RTOI roles and responsibilities as future capabilities, concepts, and Tactics, Techniques and Procedures (TTPs) become operationally available. Wherever this instruction is inconsistent with current contracts that support AFSPC's cyberspace mission areas, the contract shall govern but shall be changed at the first reasonable opportunity to comply with this instruction. Ensure that all records created as a result of processes prescribed in this publication are maintain IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule. Send comments and suggested improvements on an AF Form 847,

From section 3.1. RTOI Overview:

"24 AF/CC may exercise authority to utilize organic assets, resources and funding … in order to generate tailored applications, tools, and/or non-materiel solutions for existing weapon systems and platforms as needed."

From section 3.6. RTOI Project Qualifications:

3.6.1. Total anticipated investment must be less than $2.0M in Fiscal Year (FY) 2010 (FY10) dollars, adjusted for inflation.

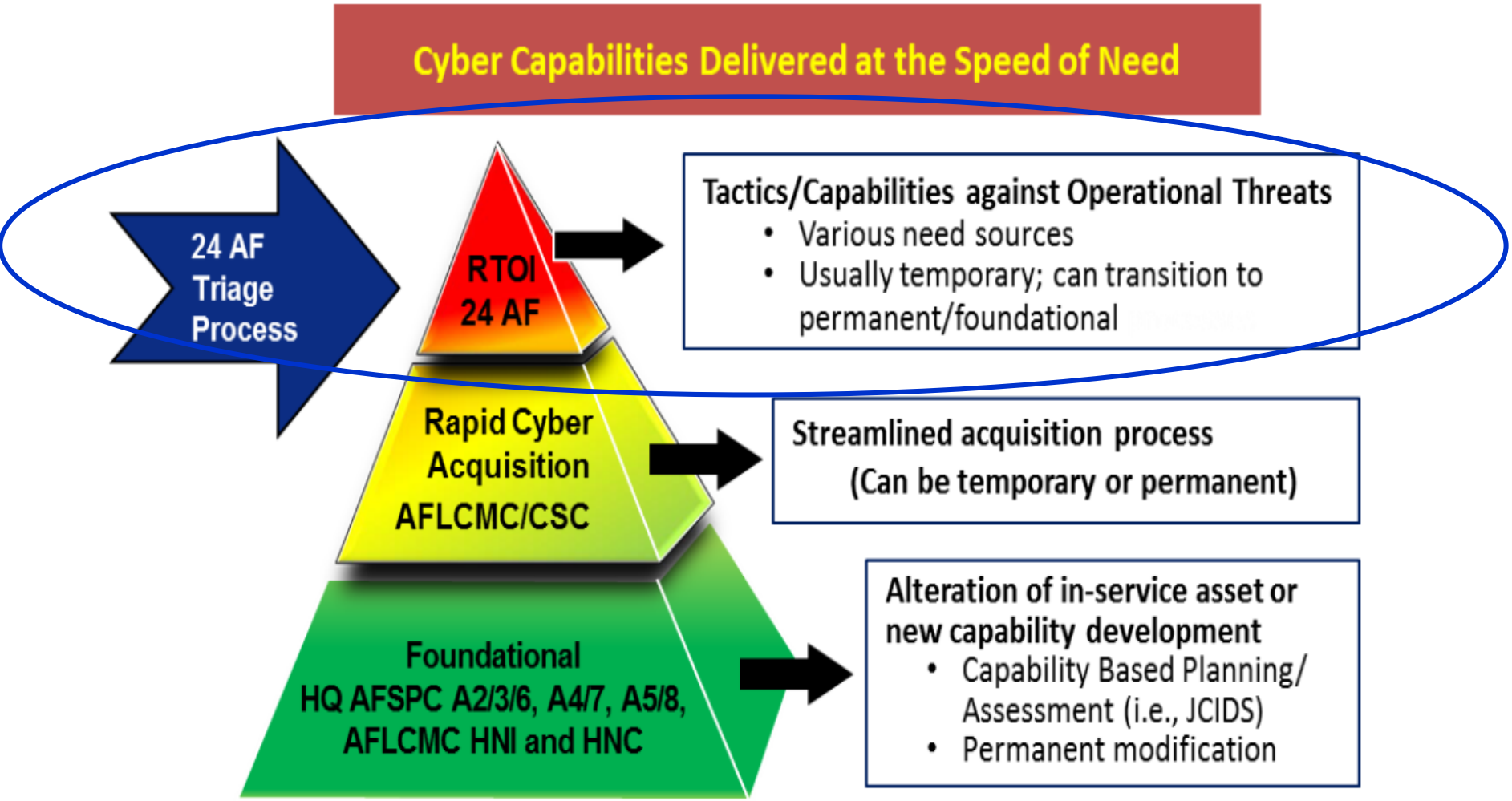
3.6.2. The candidate project enhances and/or is linked to an existing operational system, platform or capability.

3.6.3. The project's end product or capability can achieve Capability Release for Operational Use in less than 180 days from RTOI approval.

From section 4.1. Authority:

"The Capability Release Authority for Operational Use for capabilities generated under RTOI Type 1 and Type 2 processes described herein is delegated to 24 AF/CC."

For Those Who Love Pictures



AF Construct for Cyber Capability Delivery

AFSPCI10-170 1 JULY 2015, pg. 3

Debunking RTOI Myths

RTOI is **NOT An acquisition authority**

- RTOI activities are operational in nature
- RTOI activities complement AQ activities, they do not compete with them

RTOI is **NOT A specific 90 COS development process**

- Commercial/academic may feed RTOI development & release

RTOI is **NOT An independent effort**

- Operator involvement req'd (needs/capability; development/release)
- SPO involvement to enable WS integration, config mgmt & sustainment
- Test involvement is required to inform risk decisions (design thru release)
- Training & TTPs for operational employment

Validating RTOI Truths

RTOI **<u>Is</u> A capability release authority**

- Authority delegated to 24 AF/CC for operational use
- Enables prompt fielding of mission-enabling, urgent needs to meet operational requirements

RTOI **<u>Is</u> An alternate means to manage *and accept* risk**

- There is a different risk calculus in cyberspace
- Sometimes the greater risk is delay in fielding
- Assessment/testing still involved to provide informed decision
  - Must be responsive & rapid

RTOI **<u>Is</u> An innovation enabler**

- Agility of the release process enables development based upon emerging threats and/or technologies

What Qualifies as RTOI

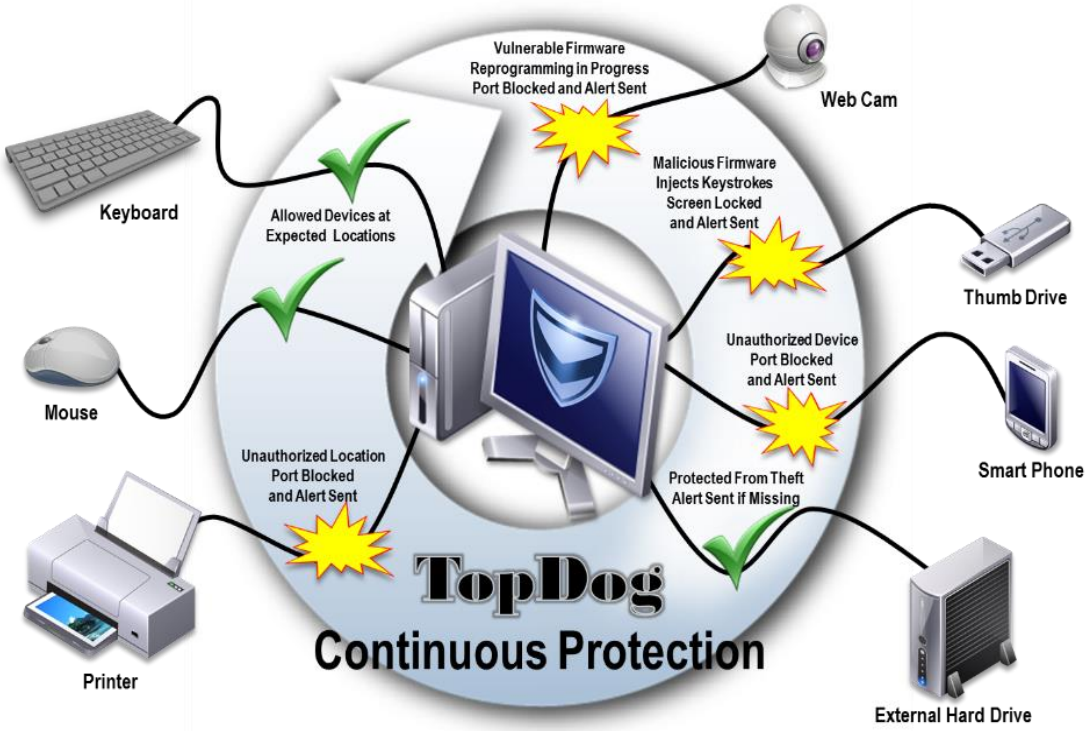
RTOI Criteria: RTOI activities are specifically intended to satisfy **critical and short-term** (180 days or less) **operational needs** in response to:

- Emergent threats and opportunities as determined by 24 AF/CC
  - 24 AF/A8/9 manages oversight of priorities

- Critical cyberspace operational needs for more effective employment of existing weapon systems (both defensive and offensive), which 24 AF/CC has been tasked to fulfill or which have been identified through the conduct of daily operations

RTOI Capability Example

- TopDog is software that counters advanced Bad-USB and similar threats: device reprogramming and Trojan functions. It augments conventional malware detection / remediation.
- Detects unauthorized devices and deeply inspects functionality, attachment location, traffic, and device counts.
- Rule-based and configuration-driven: no hard-coded policy.
- Currently provides 5 configurable real-time reactions including deny, alert, and/or lock.
- Can import specific rules and devices, and auto-detect baseline whitelist on install.



Opportunities to Improve RTOI

- Funding via Unfunded Requirements
- DevLan accreditation
  - Cumbersome RMF process for development networks
- DevOps Facility Space for Agile development teams
- Mission Partners
  - Developers / Testers / Operators
- Talented Workforce & Retention

Predominately Inherently Governmental

The 90th Cyberspace Operations Squadron has delivered 42 tailored cyber capabilities over the past 24 months via RTOI

- We've shared our processes with our Sister Services
- **Now we're pushing to find other means to deliver capabilities using RTOI**

RTOI – The Future

Industry

CRADAs

RTOI & YOU!

Partnerships

Academia

Questions / Comments / Discussion