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,

Recommendation for Change of Publication, through appropriate command channels to HQ AFSPC/A2/3/6W, 150 Vandenberg Street, Suite 1105, Peterson AFB, CO 80914 with an informational copy to 24 AF (as appropriate). Organizations requesting document changes will ensure all units that could be affected by the change are included as informational addressees. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Managemen*t, Table 1.1 for a description of the authorities associated with the Tier numbers. Submit requests for waivers through appropriate command channels to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. Whenever Tier 3 authorities grant waivers, notify HQ AFSPC/A2/3/6W. Subordinate organizations are encouraged to supplement this instruction. Supplements shall not lessen the requirements nor change the basic content or intent of this instruction. Coordinate all supplements with appropriate Major Command (MAJCOM) Offices. This Instruction is to be used in conjunction with AFI 10-601_AFSPCSUP, *Operational Capability Requirements Development;* AFI 61-101_AFSPCSUP, *Management of Science and Technology*; AFI 63-101/20-101, Integrated Life Cycle Management*;* AFI 63-131, *Modification Management;* AFI 65-601, Volume I, *Budget Guidance and Procedures;* and AFI 99-103, *Capabilities Based Test and Evaluation.*

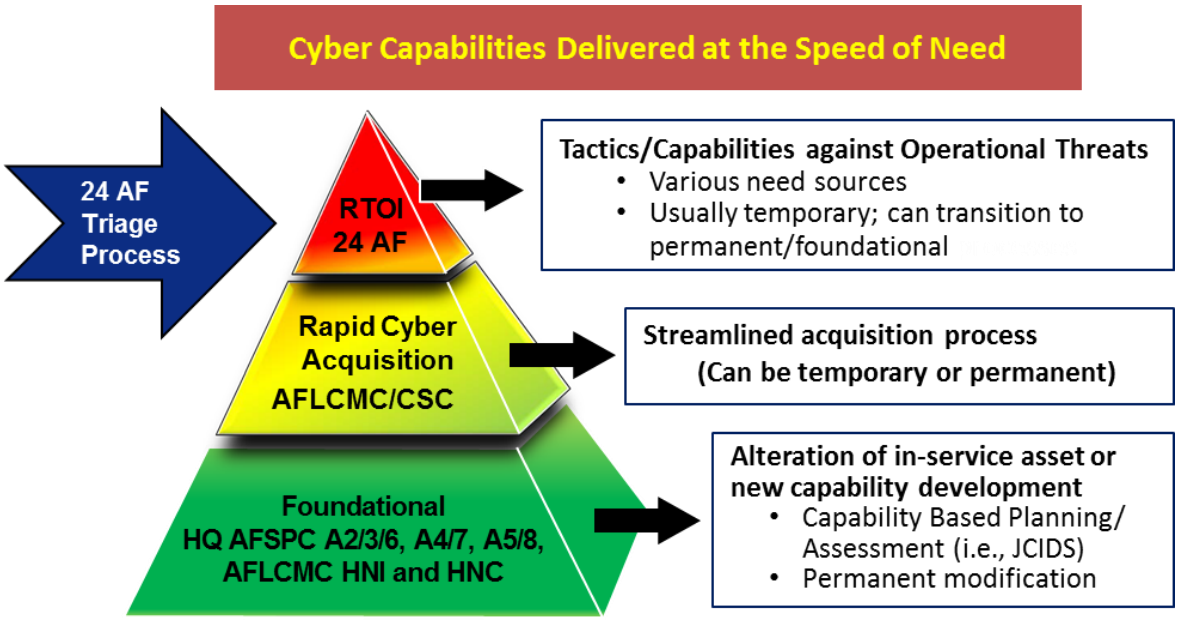
Chapter 1

GENERAL

1.1. RTOI Context. This instruction establishes roles, responsibilities, authorities, relationships, and high-level processes for executing RTOI activities.

1.2. Construct for Cyber Capability Delivery. This instruction implements the operational portion of the AF Construct for Cyber Capability Delivery ("the Construct"), which is comprised of three inter-dependent Levels of Activity, or ways to change or modify a system (**Figure 1**): Level 1, RTOI (critical and/or time-constrained mission-essential cyber capabilities and tactics improvements executed with AFSPC/24 AF operational resources); Level 2, Rapid Cyber Acquisition (RCA – accelerated acquisition of cyber capabilities) and Level 3, Foundational (conventional acquisition processes conducted within existing DoD and AF guidance).

Figure 1.1. AF Construct for Cyber Capability Delivery



Chapter 2

SCOPE, ROLES AND PROCESSES

2.1. Scope. The scope of this instruction encompasses only operational modifications to and/or enhancements of existing AF cyber systems, software, databases and networks. Within the framework provided by the Construct, HQ AFSPC/A2/3/6 is responsible for establishing proper roles, responsibilities and legitimate authorities needed to accomplish RTOI (Level 1) activities properly with AFSPC operational resources. This instruction describes these roles, responsibilities, and authorities, as well as the triage process which Commander, 24 AF (24 AF/CC) will establish and use to determine the proper Cyber Capability Delivery Level for any given change or modification project.

2.2. Roles and High-Level Processes. 24 AF/CC will develop formal processes to ensure that the Construct's triage process is applied continuously during an RTOI project's life cycle. For example, 24 AF/CC may determine that certain projects initiated under RTOI have multiple uses, warrant extended operational lifecycles, or fall outside of RTOI eligibility, as described herein. In such cases, the task of transitioning these projects to RCA (Level 2) or Foundational Acquisition processes (Level 3) is the shared responsibility of HQ AFSPC A4/7, A5/8, 24 AF, and AFLCMC. These systematic review and assessment processes enable rapid response times while maintaining thorough requirements analysis and resource prioritization in assigning a candidate project to the appropriate level. The scope of this AFSPCI does not extend to execution of existing or proposed acquisition processes which pertain to RCA. RTOI activities are subject to applicable United States Code (USC), DoD and AF financial and acquisition directives.

Chapter 3

RTOI OVERVIEW, CRITERIA AND OPERATIONAL CONSIDERATIONS

3.1. RTOI Overview. RTOI is a dynamic, agile, risk-management-based problem-solving approach, balancing critical operational cyber mission needs against other organizational resource requirements and priorities. "Innovation" in this context means proactive capability improvement in response to mission-critical cyber operational and deployment needs. RTOI projects are operational rather than acquisition-related activities. Driven by the rapidity with which cyber operational needs and vulnerabilities emerge, RTOI processes provide a flexible framework for innovative solutions to urgent cyber needs. Within this framework, 24 AF/CC may exercise authority to utilize organic assets, resources and funding (supplemented by additional funding in special cases – see **paragraph 3.4**) in order to generate tailored applications, tools, and/or non-materiel solutions for existing weapon systems and platforms as needed. When TTP development or modification is required, the RTOI processes will inform the tactics development process as defined by AFSPCI 10-260, *Tactical Development Program*. RTOI processes enable effective operational response to emergent threats or opportunities at a much faster pace than is possible using foundational acquisition processes.

3.2. RTOI Criteria. RTOI activities are specifically intended to satisfy critical and short-term (180 days or less) operational needs in response to: Cyber Incidents/Events Category 0 thru 9, as outlined in the Chairman of the Joint Chief of Staff (CJCS) Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), and CJCS Manual 6510.01B, Cyber Incident Handling Program.

3.2.1. Emergent threats and opportunities as determined by 24 AF/CC.

3.2.2. Newly discovered critical vulnerabilities not currently mitigated within the Air Force Enterprise network or capable of remediation by other means.

3.2.3. 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.

3.3. Project Nomination. Candidate projects proposed in response to documented cyber platform needs/ requirements or identified vulnerabilities can be nominated for RTOI by many AF or DoD sources; for example, DoD/Higher Headquarters (HHQ) and agencies, United States Cyber Command (USCYBERCOM), 24 AF and/or its subordinate units; and Combatant Commanders (CCDRs). Emerging cyber needs can also be conveyed to 24 AF in different ways, such as by direction of the Secretary of Defense (SECDEF) or Chief of Staff of the Air Force (CSAF), through Operations Directives (OPDIRs), Planning Orders (PLANORDs), Execute Orders (EXORDs), Cyber Tasking Orders (CTOs), Urgent Operational Needs (UONs) statements; Joint UONS (JUONs); Joint Emergent Operational Needs (JEONs); Evaluation Request Messages (EReqMs); AF Forms 1067, *Modification Proposal*, and/or 24 AF CNFs. All such cyber need nominations will be reviewed by 24 AF/CC (or his/her designated representative) to determine whether RTOI is an appropriate implementation approach.

3.4. RTOI Funding. RTOI is inherently an Operations & Maintenance (O&M) activity, so HQ AFSPC usually provides only O&M funding for RTOI projects. However, this O&M focus does not necessarily preclude the use of Research, Development, Test & Evaluation (RDT&E)

funding to support other customers using 3600 funding on their contracts, if provided as "other source funding" on a non-interference basis. **(T-2).**

3.5. RTOI Project Types. There are two RTOI project types:

3.5.1. Type 1. *Immediate Needs.* Type 1 RTOI projects address urgent mission-critical Offensive Cyberspace Operations (OCO), Defensive Cyberspace Operations (DCO) and/or DoD Information Network (DODIN)/Air Force Information Networks (AFIN) operational needs. The products of Type 1 projects are typically improved or enhanced capabilities generated in response to emerging or unforeseen operational mission needs within a pre-determined timeframe, usually measured in hours or days. Type 1 projects are considered closed when their products are either approved for inclusion in the RTOI Products and Applications Repository (the Repository) and entered in the RTOI Project Registry (the Registry), or when the operational need they were intended to satisfy no longer exists.

3.5.2. Type 2. *Known Short-term Future Needs.* RTOI projects of this Type generate capabilities to meet critical future threats or known vulnerabilities identified by Intelligence, Surveillance and Reconnaissance (ISR) or Operational Preparation of the Environment (OPE) activities, and/or provide mission assurance/risk mitigation in anticipation of future OCO, DCO and/or DODIN Operations. Type 2 RTOI projects typically focus on generating applications and/or tools in response to adversary target sets identified by AF and joint warfighters, or code/capabilities/ improvements required for near-term (usually less than one year) operational use. Prior to active combat operations, Type 2 RTOI projects will likely comprise a majority of RTOI efforts, anticipating future cyber needs in time to react effectively and arm cyber units with appropriate weapons and cyber applications in advance of mission tasking. However, such anticipatory RTOI efforts are approved only after due diligence by 24 AF leadership using internal 24 AF triage processes (see **paragraph 3.7**), considering likely future cyber taskings, emerging operational priorities, available resources, and expedited processes for rapid Technology Transition of cyber-related S&T initiatives to operational status IAW AFI 61-101, *Management of Science & Technology*. By accelerating operational implementation of platform improvements, ISR collection capabilities and threat response to cyberspace's extreme "speed of need," Type 2 RTOI projects effectively complement less-responsive RCA and foundational acquisition processes.

3.5.3. 24 AF/CC will ensure that Type 1 and/or Type 2 RTOI products' readiness for operational use is assessed according to a test strategy that takes into consideration the RTOI product's level of complexity, breadth of application, urgency of operational need, and an acceptable level of risk. When time permits, test methods chosen for RTOI products' assessment must adhere to existing Air Force and HQ AFSPC policy and guidance. For example, assessment of an RTOI product could be effectively accomplished either as a Force Development Evaluation (FDE) or by means of the Capabilities and Limitation (C&L) Report methodology presented in the current AFI 99-103 and AFSPCI 99-103, *Capabilities-Based Test and Evaluation of Space and Cyberspace Systems* documents. If time is particularly critical, Beta versions of RTOI capabilities and/or products may be released to operational cyber units before testing is complete, with documented capability analysis and acceptance of risk. RTOI projects which are complete, released for operational use (see **paragraph 4.1**), and their approved products entered into the Registry/Repository, but do not require sustainment while awaiting operational employment, may be retained indefinitely at the discretion of 24 AF/CC.

3.6. RTOI Project Qualifications. 24 AF/CC shall use the following measures to decide whether an activity falls within the scope of Type 1/Type 2 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. **(T-2)**.

3.6.2. The candidate project enhances and/or is linked to an existing operational system, platform or capability. **(T-2)**.

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. If an otherwise qualifying RTOI project is delayed beyond 180 days from approval for unforeseen operational reasons, 24 AF/CC (or his/her designated representative) may request a waiver of this criterion from HQ AFSPC/A2/3/6. **(T-2)**.

3.7. Transition to Other Levels of the Construct. If 24 AF/CC decides an urgent operational issue does not qualify for RTOI, but confirms urgency of need, all related CNFs or AF Form 1067s shall be referred to the Cyber Solutions Cell (CSC) and/or Cyber Decision Board (CDB) for evaluation as candidates for RCA **(**See Cyber Solutions Cell Concept of Operations, July 2013). AF Form 1067 is the official documentation method (form) for all RTOI projects which transition for permanent use as a change to a weapon system baseline. If a valid candidate project is determined not to qualify for either RTOI or RCA, 24 AF will submit to HQ AFSPC/A2/3/6W, A4/7 A4C, and A5/8 A5C an AF Form 1067 describing the proposed modification and its operational priority IAW AFI 63-131, *Modification Management*. AF Forms 1067 submitted to HQ AFSPC through the CSC/CDB process are considered validated requirements ready for engineering review and certification through the Validation/Certification Board (VCB) process. **(T-2)**.

3.8. RTOI Product Sustainment. If an RTOI project produces products which are determined to require future support or sustainment, 24 AF will submit an AF Form 1067 describing the proposed modification and need for sustainment to the AFSPC Modification Control Point IAW AFI 63-131_AFSPCSUP, *Modification Management*. **(T-2)**.

Chapter 4

RTOI CAPABILITY RELEASE FOR OPERATIONAL USE

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. 24 AF/CC may further delegate RTOI project approval and Capability Release Authority for Operational Use to an appropriate level, but no lower than Wing Commander or a comparable level on 24 AF staff (e.g. 24 AF/CV or A3).

4.2. Assessment. Designated Capability Release Authority for Operational Use shall assess operational readiness of RTOI projects and capabilities after appropriate risk mitigation activities have taken place, and shall ensure that they have satisfactorily met applicable operational effectiveness- and suitability-related requirements established by 24 AF. For all non-RTOI capabilities for operational use in AFSPC, the Operational Acceptance authority is HQ AFSPC/A23/6 or his/her designated representative, IAW AFSPCI 10-205, *Operational Transition Process.* **(T-2)**.

Chapter 5

RESPONSIBILITIES AND TASKS

5.1. 24 AF/CC will:

5.1.1. Ensure all RTOI activities are based upon valid, documented operational cyber needs. **(T-2)**.

5.1.2. Serve as decision/delegation authority for Capability Release for Operational Use of RTOI-generated capabilities. **(T-3)**.

5.1.3. Assist HQ AFSPC/A2/3/6 in developing funding strategy and advocacy for RTOI resources during the Program Objective Memorandum (POM) process. **(T-2)**.

5.1.4. Consult with HQ AFSPC/A2/3/6 if questions arise as to whether a candidate need or project qualifies as RTOI. **(T-2)**.

5.1.5. Submit RTOI Monthly Status Reports (MSRs) to HQ AFSPC/A2/3/6W, A4/7 A4C and A5/8 A5C no later than the 10th calendar day of every month. MSRs shall contain a description of each RTOI initiative, documented cyber need (CNF or AF Form 1067 reference number if applicable) or identified vulnerability, identification of existing operational system and/or platform it is linked to, status of project/innovation, status of project testing, description of completed/planned risk mitigation steps and mission assurance activities, estimated RTOI activity costs (R&D costs), and projected sustainment costs. 24 AF/CC may designate a wing or group-level organization as OPR for RTOI MSRs**. (T-2)**.

5.1.6. Establish formal internal operating instructions describing specific:

5.1.6.1. RTOI candidate project identification and tracking processes, including CNF preparation, evaluation, and management, in accordance with the provisions of this instruction. **(T-2)**.

5.1.6.2. 24 AF cyber triage processes for RTOI approval (including any delegations of approval authority). **(T-3)**.

5.1.6.3. Guidance on resource use for RTOI activities, provision of technical expertise, and appropriate RTOI-related analysis, testing, training, and/or development/modification of TTPs. **(T-3)**.

5.1.6.4. Processes for conducting Capability Release for Operational Use assessment (IAW AFPD 10-17, *Cyberspace Operations,* AFSPCI 10-205 and related AFIs) and meeting operational effectiveness and suitability criteria. **(T-3)**.

5.1.6.5. 24 AF internal processes for transitioning certain RTOI projects to RCA or Foundational Processes (as appropriate), IAW **paragraphs 2.1** and **paragraph 3.7** of this instruction. **(T-2)**.

5.1.6.6. Procedures for creating, maintaining, updating and auditing the Repository and Registry. Audits shall be performed at least annually. **(T-2)**.

5.2. HQ AFSPC/A2/3/6 will:

5.2.1. Provide policy, guidance and adjudication of issues arising from RTOI processes, and ensure integration with the Cyberspace Superiority Core Function Support Plan (CFSP). **(T-2)**.

5.2.2. Develop funding strategy and advocate for RTOI resources during the POM process. **(T-2)**.

5.2.3. Accept, review, validate and advocate for resources to support RTOI Unfunded Requirements (UFRs) proposed by 24 AF or subordinate units. **(T-2)**.

5.2.4. Ensure appropriate changes and additions are made to weapon system operations and training documents to reflect RTOI products used by or incorporated in weapon systems. **(T2).**

5.2.5. Ensure RTOI MSRs are disseminated to other HQ AFSPC Divisions and functional areas. **(T-3)**.

5.2.6. Review MSR status, resolve issues with RTOI projects, and present project management recommendations at the applicable HQ AFSPC/A2/3/6W-led Weapon System Team meetings. **(T-3)**.

5.2.7. Assist 24 AF in transitioning candidate projects which do not qualify for RTOI into RCA and/or foundational acquisition processes as appropriate. **(T-2)**.

5.3. HQ AFSPC A4/7 will:

5.3.1. Assist 24 AF and AFLCMC in transitioning proposed projects which do not qualify for RTOI into RCA or foundational delivery mechanisms (as appropriate). **(T-2)**.

5.3.2. Serve as the Modification Control Point for all 1067s, and participate in any 3400 funding discussions which involve logistic requirements and/or transition documentation. **(T2).**

5.3.3. Assist 24 AF, AFLCMC and AFSPC/A2/3/6 in determining sustainment requirements, as appropriate. **(T-2).**

5.4. HQ AFSPC A5/8 will:

5.4.1. Assist HQ AFSPC A2/3/6 in developing funding strategy and advocacy for RTOI resources during the POM process. **(T-2)**.

5.4.2. Assist 24 AF in transitioning warfighter needs (which do not qualify for RTOI or RCA processes) into foundational delivery mechanisms (if appropriate). **(T-2)**.

5.4.3. Review MSR status; assist in resolving issues with RTOI projects, and present project management/requirements recommendations at applicable Integrated Concept Team (ICT) meetings. **(T-2)**.

5.4.4. Ensure appropriate changes and additions are made to weapon system requirements to reflect RTOI products used by or incorporated in weapon systems. **(T-2)**.

5.5. 24 AF and/or subordinate units will:

5.5.1. Develop and promulgate appropriate changes and additions to tactics bulletins, TTPs, and other operational procedures for each RTOI capability accepted for operational use IAW

AFI 11-260, *Tactics and Development Program* and AFI 11-415, *Weapons and Tactics Programs*. **(T-3)**.

5.5.2. To the extent feasible before beginning an RTOI activity, coordinate with HQ AFSPC and external organizations such as AFLCMC/HN, AFTENCAP, and AFRL to minimize duplication of effort and ensure efficient use of resources. Action Officer-level coordination and/or direct liaison among participating AFSPC organizations is encouraged. Contact points for such inquiries are: AFLCMC/HNC, Cyber Solutions Cell; USAFWC-AF TENCAP/TCE, Office: 719-567-0480 (DSN 560), Secure VoIP: 980-1528; and AFRL/RIG, **afrl.rigm@us.af.mil.** **(T-3)**.

5.5.3. Ensure all completed RTOI projects follow 24 AF procedures for Capability Release for Operational Use. Testing shall be conducted in an appropriate operational test environment and adhere to established test and evaluation standards. Risk assessment/management analyses shall be conducted throughout the duration of each RTOI project in accordance with National Institute of Standards and Technology Special Publication 800-30, Revision 1 and AFPD 90-8, *Environment, Safety & Occupational Health Management and Risk Management*. **(T-2)**.

5.5.4. Submit UFR package to HQ AFSPC/A2/3/6W for RTOI projects which need additional support beyond 24 AF organic resources. UFR packages will describe the specific RTOI project, linkage to existing capability or weapon system, impact if not funded, CNF number (if applicable), and any other appropriate supporting documentation (e.g., JUONS, Vulnerability Assessments and/or Plans of Action and Milestones (POA&Ms)). **(T-2)**.

5.5.5. Ensure each released RTOI product or capability is placed in the Repository, listed in the Registry and that appropriate information is released to the USCYBERCOM Cyber Capabilities Registry (CCR). **(T-2)**.

5.5.6. Ensure feedback is provided to appropriate organizations following testing, approval, and operational employment of each RTOI product or capability. **(T-3)**.

5.5.7. Ensure Weapon System Team (WSTs) update necessary Concept documents, weapon system configuration baseline(s), and/or maintenance documentation if a capability generated under RTOI requires sustainment. 24 AF and or subordinate units shall coordinate updates of Weapon System Operations Concepts, weapon systems baselines, sustainment requirements, etc. with the appropriate WST Lead. **(T-3)**.

5.5.8. If transition of RTOI activity to RCA or foundational processes is necessary, coordinate closely with HQ AFSPC A4/7 and AFLCMC, and follow **paragraph 3.7** of this instruction. Submit an AF Form 1067 for all RTOIs/CNFs that will require future support and sustainment IAW AFI 63-131, Modification Management. **(T-2)**.

Chapter 6

RTOI RECORDS MANAGEMENT

6.1. Caveats. Draft documents released prior to HQ AFSPC approval must clearly state that they do not necessarily reflect AFSPC policy or approval and are subject to change. **(T-2).**

6.2. Agreements. When required, ensure appropriate formal RTOI agreements are documented and approved by all organizations and agencies which may participate in RTOI projects. Agreements will outline roles, responsibilities and authorities among all affected operational, supporting and external organizations. **(T-3).**

STEPHEN T. DENKER, Major General, USAF
Director of Integrated Air, Space, Cyberspace and ISR Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

CJCS Instruction 3170.01I, *Joint Capabilities Integration and Development System (JCIDS),* 23 January 2015

CJCS Instruction 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND),* 9 February 2011 (current as of 10 Oct 2013)

CJCS Manual 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments,* September 2012

AFPD 10-17, *Cyberspace Operations*, 31 July 2012

AFPD 90-8, *Environment, Safety & Occupational Health Management and Risk Management*, 2 February 2012

AFI 10-601_AFSPCSUP, *Capabilities Based Requirements Development*, 10 June 2014

AFI 11-260, *Tactics Development Program*, 15 September 2011

AFI 11-415, *Weapons and Tactics Programs,* 15 October 2014

AFI 33-360, *Publications and Forms Management,* 25 September 2013

AFI 61-101_AFSPCSUP, *Management of Science and Technology,* 23 October 2013

AFI 63-131, *Modification Management*, 19 March 2013

AFI 99-103, *Capabilities-based Test and Evaluation*, 16 October 2013

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSPCI 10-205, *Operational Transition Process,* 10 December 2013

AFSPCI 10-260, *Tactical Development Program,* 28 November 2011

AFSPCI 99-103, *Capabilities-Based Test and Evaluation of Space and Cyberspace Systems,* 20 December 2010

Cyber Solution Cell Concept of Operations, July 2013

Prescribed Forms

This supplement does not contain any prescribed forms.

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

AF Form 1067, Modification Proposal

Abbreviations and Acronyms

24 AF—Twenty-Fourth Air Force

24 AF/CC—Commander, 24 AF

AF—United States Air Force

AFI—Air Force Instruction

AFIN—Air Force Information Networks

AFLCMC—Air Force Life Cycle Management Center

AFMAN—AF Manual

AFPD—Air Force Policy Directive

AFSPC—Air Force Space Command

AFSPC/CC—Commander, AFSPC

ARC—Air Reserve Component

CCDR—Combatant Commander

C&L—Capabilities and Limitation

CCR—Cyber Capabilities Registry

CDB—Cyber Decision Board

CFSP—Core Function Support Plan

CJCS—Chairman of the Joint Chiefs of Staff

CND—Computer Network Defense

CNF—Cyber Needs Form

CSAF—Chief of Staff of the Air Force

CSC—Cyber Solutions Cell

CTO—Cyber Tasking Order

DCO—Defensive Cyberspace Operations

DoD—Department of Defense

DODIN—DoD Information Networks

DOTMLPF-P —Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

EReqM—Evaluation Request Message

EXORD—Execute Order

FDE—Force Development Evaluation

FMRs—Financial Management Regulations

FY—Fiscal Year

HHQ—Higher Headquarters

IA—Information Assurance

IAW—In accordance with

ICT—Integrated Concept Team

ISR—Intelligence, Surveillance, and Reconnaissance

JCIDS—Joint Capabilities Integration Development System

JEON—Joint Emergent Operational Need

JUON—Joint Urgent Operational Need

MAJCOM—Major Command (AF)

MDA—Milestone Decision Authority

MDD—Materiel Development Decision

MSR—Monthly Status Report

O&M—Operations & Maintenance

OCO—Offensive Cyberspace Operations

OPDIR—Operations Directive

OPE—Operational Preparation of the Environment

OPR—Office of Primary Responsibility

PLANORD—Planning Order

POM—Program Objective Memorandum

POA&M—Plan of Action and Milestones

RDT&E—Research, Development, Test & Evaluation

RTOI—Real-Time Operations and Innovation

S&T—Science and Technology

SECDEF—Secretary of Defense

TTPs—Tactics, Techniques and Procedures

UFR—Unfunded Requirement

UON—Urgent Operational Need

USC—United States Code

USCYBERCOM—United States Cyber Command

VCB—Validation/Certification Board

WST—Weapon System Team

Terms

Approval—Approval signifies agreement/acceptance/coordination by a duly authorized AFSPC official IAW AFSPC/24 AF Instructions and/or Memoranda of Agreement.

Capabilities and Limitations (C&L) Report—An optional, quick-look report of limited scope that operational testers provide to operational units to support rapid and/or early fielding of developing capabilities before dedicated operational testing is complete and formal production begins. It provides the most current operational test perspectives on system capabilities and limitations based on testing done to date, and describes any untested or unknown areas. **NOTE:** Reference AFI 99-103, pg 85.

Capability—The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. **NOTE:** Reference CJCSI 3170.01G. In this instruction, the intended meaning is a materiel or non-materiel enhancement applied to an existing weapon system or application set to enable effective response to an urgent operational need or emergent threat.

Existing—In being; currently in operational service; post-OA (systems).

Force Development Evaluation—A type of dedicated OT&E performed by MAJCOM Operational Test Organizations in support of MAJCOM-managed system acquisition-related decisions and milestones prior to initial fielding, or for subsequent system sustainment or upgrade activities. An FDE may be used for multiple purposes to include:

a) Evaluate and verify the resolution of previously identified deficiencies or shortfalls, including those rated in AFOTEC reports as not having a substantial or severe impact on mission operations.
b) Evaluate routine software modifications (e.g., operational flight programs (OFP)), subsequent increments, upgrades, and other improvements or changes made to sustain or enhance the system.
c) Evaluate and verify correction of new performance shortfalls discovered after fielding of the system.
d) Evaluate operational systems against foreign equipment.
e) Evaluate operational systems against new or modified threats.

f) Evaluate military—unique portions and applications of COTS, NDI, and GFE for military use.

Innovation—Proactive capability improvement in response to mission-critical (cyber) operational and deployment needs.

Near-term—Usually less than 1 year.

Real Time Operations and Innovation—Operational activities which produce critical and/or mission-essential cyber weapon system/platform modifications, capability improvements, and related changes to operational procedures at the "speed of need."

Short-term—180 days or less.

Triage—Sorting and allocating resources on the basis of need for or likely benefit from immediate and/or urgent response and/or corrective action (evolving cyber usage). In software triage generally, the context is "a system used by software development teams to ration limited technical resources when the number of defects needing resolution exceeds the resources available to correct and verify them so as to resolve the greatest number of defects possible." **NOTE:** Reference **http://www.stickyminds.com/article/software-triage?page=0%2C0**. However, in the sense that "triage" is used in this instruction, the controlling analytical criteria

are first, mission/time criticality, and second, whether the need or issue can be addressed successfully with locally-available resources.

Verify—To review, inspect, test, check, measure, audit or otherwise confirm that products, processes, or documents conform to specified requirements.

Year—As used herein, the term "year" refers to a 12-month interval.