Annex A (Course Credit Criteria) to the Cyber School Course Credit Program SOP

Module	AOC/MOS	Pre-approved Constructive/Equivalent Credit Criteria
Joint Cyber Analysis Course (JCAC)	17C	Credit granted with CCTC completion Understanding and application of KSAs as identified on: https://www.milsuite.mil/wiki/Joint_Cyber_Analysis_Course_Self_Study
Cisco Certified Network Associate (CCNA)	17A	Current CCNA Routing and Switching ***or*** ICND1/ICND2 certification ***or*** minimum of three credit hours of undergraduate or graduate level networking
Certified Information Systems Security Professional (CISSP)	17A	Current CISSP certification ***or*** successful exam completion with associate of ISC2
Programming	17A 17C	College Semester of Python ***or*** Example of programs written in Python (can be submitted on JWICS) ***or*** PCAP certification Demonstrated proficiency in Bash, PowerShell, & Python
Cyber Common Technical Core (CCTC)	17C 17A	ICC ***or*** Alt-ICC ***or*** OSCP
Cyber Protection Team-Core Methodologies	17C 17A	Proof of CPT 17-series Work Role Qualification
Offensive Cyberspace Operations (OCO) Analyst Core	17C	ADET/NCS Resident Courses: CYEC2200, CRSK1000, NETW1002, NETA1030 ***and*** CBTs: OVSC1100, OVSC1700, OVSC1203, OVSC1800, CYEC1200, CYEC1250, CYEC2050, NETA2002, RPTG1012, TOOL2201, SIGC2700 ***or*** Proof of CMT 17-series (DNEA or EA) Work Role Qualification
Joint Advanced Cyber Warfare Course – Georgia (JACWC-G)	17A	JACWC ***or*** PACWC
Cyber Operations Planners Course (COPC)	17A	JCOPC, ACOPC, ***or*** JNAC
Cyberspace Response Assessment (CsRA)	17C 17A	Documented USCC or CNMF Exercise Participation (RED or BLUE cells only) ***or*** Deployment as Cyber Planner/Operator/Analyst with 2x CTC or 2x DIV/CORPS War Fighter Exercise in documented cyber role (non- signal/military intelligence position) ***or*** a crosswalk from the individual demonstrating how they have met the 13 CsRA ELO requirements
Tier I Forensics Triage	170A	"GIAC GCFE ***or*** ECC CHFI ***or*** DCITA FIWE
Incident Response	170A	GIAC GCIH ***or*** GIAC GDAT ***or*** GIAC GCFA ***or*** ECC ECIH ***or*** InfoSec Incident Response and Network Forensics Course ***or*** DCITA CIRC
Networking Devices	170A	CCNA R&S ***or*** CCNA Security ***or*** CCNP R&S ***or*** CCNP Security ***or*** CCIE R&S ***or*** CCIE Security ***or*** CCTC 2018 or earlier ***or*** ICC ***or*** ALT-ICC ***or*** DCITA LNI ***or*** JCAC
Regular Expressions	170A	CCTC 2018 or earlier ***or*** ICC ***or*** ALT-ICC ***or*** JCAC
Hacking Methodologies	170A	OSCP ***or*** OSCE ***or*** GIAC GPEN ***or*** GIAC GXPN ***or*** ECC LPT ***or*** T10 Operators Course ***or*** DCITA CTE Methodologies Course
Enterprise Networks	170A	GIAC GCED ***and*** GIAC GSNA ***or*** CCDA and CEH
Scripting: Python	170A	GIAC GYPC ***or*** JCAC

Annex A (Course Credit Criteria) to the Cyber School Course Credit Program SOP

Scripting: PowerShell	170A	GIAC GCWN ***or*** JCAC ***or*** Microsoft PowerShell Certification or DoD Service Training Center PowerShell Training Certificate 40 hours or more (no CBT or online)GIAC GYPC ***or*** JCAC
Traffic and Protocol Analysis	170A	GIAC GCIA ***or*** GIAC GNFA ***or*** ECC CND
Joint and Army Doctrine Block 1	170A	ACOPC ***or*** COPC ***or*** JCOPC ***or*** JNAC ***or*** AIOPC
Joint and Army Doctrine Block 2	170A	Army Mission Commander Course
Defensive Operations	170A	(DCITA DCI Methodologies OR CPB Circadence Table IV Certification) and Tier I Forensics Triage Equivalency and Incident Response Equivalency and Scripting: PowerShell Equivalency and Traffic and Protocol Analysis Equivalency
Offensive Operations	170A	T10 Operators course ***or*** RIOT

NOTES:

1. Training which produces a certificate requires either a Certificate or a validated test result showing the passing of the certification.

2. For certification training (i.e., CASP, CCNA, CISSP), students attending a course at the Cyber School must present a current certification at the start of their overall course (i.e., BOLC, CyOOC).

3. The above pre-approved course credit criteria is not necessarily all-inclusive and focuses on constructive and equivalent credit; credit for operational experience is calculated on a case-by-case basis using applicant-provided documentation.

4. 170A WOBC is awarded in full or not at all; there is no partial equivalency for the course. Packets must meet equivalency for at least 11/14, including the Defensive and Offensive Operations modules, or more within WOBC for acceptance. Otherwise, students must attend and successfully graduate from the course. All Warrant Officer Candidate School (WOCS) graduates who have not completed a WOBC must complete WOBC as part of the Warrant Officer Commissioning process. As such, all WOCS graduates who have not completed a WOBC will be required to attend 170A WOBC regardless of previous education, training, or operational experience.

5. There are currently no criteria established for 17E, 17B, or 170B course credit. Determinations will be made initially on a case-by-case basis until a baseline is established.