ARTICULATION AGREEMENT BETWEEN DEPARTMENT OF DEFENSE CYBER CRIME CENTER (DC3) AND STEVENSON UNIVERSITY

This Articulation Agreement ("Agreement") is made by and between Department of Defense Cyber Crime Center ("DC3"), 911 Elkridge Landing Road, Linthicum, MD 21090, and Stevenson University, 1525 Greenspring Valley Road, Stevenson, MD 21153 (hereafter referred to as "the Parties").

To better serve students intending to pursue careers in cybersecurity within the Department of Defense (DoD), and to better serve those within the DoD with a cybersecurity skillset to attain college credit towards a formal university degree, Stevenson University and DC3 Cyber Training Academy ("CTA") share a common interest in facilitating the smooth transition of students transferring from CTA to Stevenson University.

CTA designates national Centers of Digital Forensics Academic Excellence ("CDFAE") to establish best practices for digital forensics education. CDFAE is a partnership between academia, standards bodies, and the U.S. Government to establish best practices for digital forensics education. Education providers are held to digital forensics education standards based upon knowledge, skills, and abilities ("KSA") used in the field. This approach advances the discipline of digital forensics and increases the number of qualified professionals to meet the needs of law enforcement, counterintelligence, national defense, and legal communities.

CDFAE recognizes two certifications, the Digital Media Collector and the Digital Forensic Examiner. The courses articulated in this document relate to courses required by these two certifications.

The parties hereto agree to offer an articulated program pathway leading to relevant DoD certifications to be provided by CTA for Stevenson University students who have successfully completed courses in the program pathway leading to the award of a B.S. in Cybersecurity and Digital Forensics.

While DC3 and Stevenson University do not presently have a dual enrollment program, should one be agreed to, this agreement will not preclude students from participation and students may apply for and receive the benefits of dual enrollment. Those students would then be subject to the policies of said program should they apply.

Now, **THEREFORE**, in consideration of the mutual promises and conditions herein, the adequacy of which is hereby acknowledged, DC3 and Stevenson University hereby agree as follows:

The following general principles guide the operation of this agreement:

1. The program is designed for students who have been certified through DC3's Defense Cyber Training Academy (DCA). A maximum of 15 credit hours from DC3 will be allowed toward fulfillment of the 120 credit hours required for baccalaureate completion.
    a. All course credits as delineated in the attached course equivalencies will be accepted as transfer to fulfill Stevenson University requirements for the B.S. in Cybersecurity and Digital Forensics. Only courses in which the student earns a "Pass" score are eligible for transfer.
    b. Students must be in good standing at CTA in order to transfer.
    c. Students intending to transfer should complete the admission application for Stevenson University. Students should contact the Financial Aid Office at Stevenson University as soon as possible in regard to college deadlines for financial aid.
    d. DC3 students who have been certified through CTA will be given every consideration for financial assistance and will be eligible to compete for academic scholarships at Stevenson University.

e. Students who begin their studies at DC3 will be treated on an equal basis with students who began their studies at Stevenson University in regard to the award and distribution of financial aid, campus housing, course selection, registration and all other student services.
f. Students must follow all enrollment and graduation procedures in accordance with Stevenson University policy. Summary of articulated credits, current credit awards, and program requirements are set forth in Exhibit A incorporated herein and made a part of this Agreement.
g. Every student completing courses at Stevenson University will be recognized as having completed the equivalent CTA courses/training for the purpose of receiving relevant DoD certifications.

2. This program is also designed so that students in Stevenson's BS in Cybersecurity and Digital Forensics will receive a CDFAE (Center of Digital Forensics Academic Excellence) Certificate of Completion once they have completed all degree program requirements. Stevenson University will present the student with the certificate and instructions for receiving corresponding CTA digital forensics certifications.
3. DC3 and Stevenson University further agree to monitor the performance of this agreement and to revise it as necessary.
4. Appointed institutional representatives at DC3 and Stevenson University will ensure that appropriate personnel in their respective institution are aware of this agreement, including the admissions and advising staffs, transfer coordinator, and appropriate faculty and deans.
5. Stevenson University or DC3 may publicize this agreement. DC3 will identify Stevenson University as being among the institutions with articulation agreements in any information it provides to DCA students who may be interested in pursuing a bachelor's degree in Cybersecurity and Digital Forensics.
6. Any curriculum modification by either party affecting more than 25% of the curriculum must be conveyed within three (3) months of the modification in writing by:
    a. CTA to Stevenson University through the Signatories at Stevenson University, or by
    b. Stevenson University to the CTA through the chair of the DC3 Academic Cyber Curriculum Alliance.
7. DC3 and Stevenson University will review the agreement every three years.

This agreement becomes effective upon signature by all parties and shall continue in effect unless voided by either party upon sixty (60) days prior written notice. DC3 and Stevenson University will consider, in good faith, any amendments proposed by either party; however, the agreement may only be amended in writing, signed by both parties.

The agreement may be terminated by either party for due cause or after adequate notice to the other. Termination of the agreement will not affect any students currently enrolled at DC3 at the time of termination, and they shall be able to transfer credits pursuant to this agreement.

Attachment Exhibit A

IN WITNESS WHEREOF Duly authorized representatives of Stevenson University and DC3 executed this agreement as of the dates given below.

Susan T. Gorman Digitally signed by Susan T. Gorman Date: 2020.08.14 15:34:39 -04'00' — 08/14/2020

Susan Thompson Gorman, Ph.D. — Date
Executive Vice President for Academic Affairs and Provost
Stevenson University

SPECHT.JEFFREY.D.1086451553 Digitally signed by SPECHT.JEFFREY.D.1086451553 Date: 2020.08.17 14:45:34 -04'00' — 08/17/2020

Jeffrey D. Specht, SES, DAF — Date
Executive Director
Department of Defense Cyber Crime Center

This Agreement will be reviewed by both parties every three (3) years effective from the date of last signature.

Exhibit A – Summary of Articulated Courses

Students completing the following **DC3 Cyber Training Academy Courses:**	Will receive transfer credit for the following **equivalent Stevenson University courses** (All are three credits):
INCH: Introduction to Networks and Computer Hardware	IS-231: Network Technologies
ICI: Introduction to Cyber Investigations	CDF 261: Digital Forensics
LXE (Linux Essentials) *and* INCH (Introduction to Networks and Computer Hardware)	IS 231: Network Technologies and CDF 240: Linux Administration
CIRC (Computer Incident Responders Course)	CDF 391: Incident Response and Investigation
WFE-FTK or WFE-E (Windows Forensic Examinations – FTK or EnCase)	CDF 393: Forensics Evidence Collection Tools and Techniques
NIB (Network Intrusion Basics) *and* LA (Log Analysis) *and* NTC	CF 271 Advanced Network Defense

Students completing the following **Stevenson University Course:**	Will receive transfer credit for the following **DC3 Cyber Training Academy CTA** equivalent courses:
IS 231: Network Technologies	INCH: Introduction to Networks and Computer Hardware
CDF 261: Digital Forensics	ICI: Introduction to Cyber Investigations
IS 231: Network Technologies and CDF 240: Linux Administration	LXE (Linux Essentials) and INCH (Introduction to Networks and Computer Hardware)
CDF 391: Incident Response and Investigation	CIRC (Computer Incident Responders Course)
CDF 393: Forensics Evidence Collection Tools and Techniques	WFE-FTK or WFE-E (Windows Forensic Examinations – FTK or EnCase)
CF 271 Advanced Network Defense	NIB (Network Intrusion Basics)
Notes on Stevenson University Courses:	
CDF 391: Incident Response and Investigation	*Previously IS 391*
CDF 393: Forensics Evidence Collection tools and Techniques	*Previously IS 393*
CDF 261: Digital Forensics	*New course beginning Spring 2020*
CF 271: Advanced Network Defense	*New course Spring beginning 2020*

***Please Note: CTA Courses/Course Names may change over time.**

Exhibit A (Continued)

BS in Cybersecurity and Digital Forensics Suggested Course Sequence

YEAR 1				
SEMESTER	FALL		SPRING	
	INT 100 Principles of Academic Integrity	0		
	FYS 100 First Year Seminar	1		
	ENG 151 Composition & Writing from Sources	3	ENG 152 Writing about Literature and Culture	3
	CDF 110 Cybersecurity and Digital Forensics Fundamentals	3	IS 231 Network Technologies	3
	IS 140 Information Systems Architecture and Design	3	IS 240 Programming Concepts	3
	Quantitative Literacy (QL)	3-4	SEE Math or Science (SR, SR-L or QL)	3-4
	Communication Intensive (CI)	3	Humanities I* (HUM)	3
CREDITS	16 - 17 CREDITS		15 - 16 CREDITS	
YEAR 2				
SEMESTER	FALL		SPRING	
	MGT 210 Business Writing 200-level Writing Intensive (WI)	3	IS 232 TCP and IP Communication Protocols for Windows and UNIX *(offered spring)*	3
	CDF 251 Network Security	3	CDF 240 Linux System Administration	3
	CDF 252 Networking II	3	CDF 261 Digital Forensics	3
	IS 235 Advanced Windows Server Architecture & Administration	3	CDF 271 Intrusion and Penetration Testing	3
	Scientific Reasoning - Lab (SR-L)	4	CDF 281 Advanced Network Defense	3
CREDITS	16 CREDITS		15 CREDITS	
YEAR 3				
SEMESTER	FALL		SPRING	
	IS 331 Cisco TCP and IP Routing *(offered fall)*	3	IS 365 Writing for IS Applications 300/400-level Writing Intensive (WI)	3
	CDF 290 Legal Aspects of Cybersecurity	3	CDF 393 Forensic Evidence Collection Tools and Techniques	3
	CDF 391 Incident Response and Investigation	3	CDF 475 Advanced Digital Forensics	3
	CDF 392 Information Systems Forensics Internals Auditing	3	Humanities II* (HUM)	3
	Social Science I** (SS)	3	General Elective	3
CREDITS	15 CREDITS		15 CREDITS	
YEAR 4				
SEMESTER	FALL		SPRING	
	IS 432 Network Security-Firewalls, IDS, and Counter Measures	3	CDF 480 Cybersecurity and Digital Forensics Capstone	3
	Fine Arts (FA)	3	Humanities IV* (HUM)	3
	Humanities III* (HUM)	3	Social Science II** (SS)	3
	General Elective	3	General Elective	3
	General Elective	3	General Elective, if needed	3
CREDITS	**15 CREDITS**		**12-15 CREDITS**	