NCWF Categories and Specialty Areas		NIST Cybersecurity Framework Functions					Learning Objectives						
		TAWG-1	TAWG-2		TAWG-3		TAWG-2			TAWG-1		TAWG-3	
NCWF CATEGORY	SPECIALTY AREA TITLE	Identify	Protect	Detect	Respond	Recover	LO#1748 SIG-1	LO#1351 SIG-2	LO#7682 SIG-3	LO#1468 SIG-4	LO#879 SIG-5	LO#1741 SIG-6	LO#1738 SIG-7
Analyze (AN)	All-Source Analysis (ASA)			X	X		X	X				X	X
	Exploitation Analysis (EXP)		X	X	X		X	X				X	X
	Language Analysis (LNG)			X	X								
	Targets (TGT)		X	X	X		X	X				X	
	Threat Analysis (TWA)		X	X	X		X	X				X	X
Collect and Operate (CO)	Collection Operations (CLP)		X	X								X	
	Cyber Operational Planning (OPL)	X				X		X		X	X		X
	Cyber Operations (OPS)		X	X	X	X				X		X	
Investigate (IN)	Cyber Investigation (INV)				X	X						X	X
	Digital Forensics (FOR)			X	X	X		X				X	X
Operate and Maintain (OM)	Customer Service and Technical Support (STS)	X	X		X				X	X		X	X
	Data Administration (DTA)		X	X				X					X
	Knowledge Management (KMG)	X	X	X					X				
	Network Services (NET)		X	X	X	X		X		X		X	X
	Systems Administration (ADM)		X	X	X			X		X		X	X
	Systems Analysis (ANA)	X	X	X		X		X		X		X	X
Oversee and Govern (OV)	Cybersecurity Management (MGT)	X						X	X	X	X		X
	Executive Cyber Leadership (EXL)	X									X		
	Legal Advice and Advocacy (LGA)	X									X		
	Program/Project Management and Acquisition (PMA)	X			X	X				X	X		
	Strategic Planning and Policy (SPP)	X						X		X	X		X
	Training, Education, and Awareness (TEA)	X	X						X		X		X
Protect and Defend (PR)	Cybersecurity Defense Analysis (CDA)		X	X			X	X				X	
	Cybersecurity Defense Infrastructure Support (INF)		X	X				X		X		X	X
	Incident Response (CIR)				X	X		X	X			X	X
	Vulnerability Assessment and Management (VAM)	X	X	X			X	X	X	X		X	X
Securely Provision (SP)	Risk Management (RSK)	X				X	X	X	X	X	X	X	X
	Software Development (DEV)	X								X			
	Systems Architecture (ARC)	X						X		X			
	Systems Development (SYS)	X						X		X			
	Systems Requirements Planning (SRP)	X				X		X		X	X		X
	Technology R&D (TRD)	X						X		X			
	Test and Evaluation (TST)	X					X	X	X	X			

Learning Objectives - Defined

LO#1748 – Understand the fundamentals of network and application vulnerability scanners, common commercial and open source tools, and how to defend against them
LO#1351 – Understand penetration testing (PT)
LO#7682 – Explain the importance of security related awareness and training
LO#1468 – Understand processes, for managing scheduled and non-scheduled changes to the production systems and/or infrastructure including change, configuration, release and patch management practices
LO#879 – Understand and align security function to goals, mission, and objectives of the organization
LO#1741 – Understand the general approaches to get rid of the attacker's artifacts on compromised machines, the general strategy to safely restore operations, and the importance of the incident report and "lessons learned" meetings
LO#1738 – Understand what incident handling is, why it is important, and the best practices to take in preparation for an incident