

ACRONYMS

ACL - Access Control Lists	PCI - Payment Card Industry
AES - Advanced Encryption Standard	PHI - Protected Health Information
ASI - Authorized Service Interruption	PI - Proprietary Information
BGP - Border Gateway Protocol	PKI - Public Key Infrastructure
CIA - Confidentiality, Integrity, Availability	PMI - Preventive Maintenance Interruption
COOP - Continuity of Operations Plan	POAM - Plan of Actions & Milestones
DLP - Data Loss Prevention	RADIUS - Remote Authentication Dial-In Service
DNS - Domain Name Server	RFI - Request for Information
HBSS - Host Based Security System	RMA - Risk Management Assessment
IAM - Identity Access Management	RMF - Risk Management Framework
IDS - Intrusion Detection System	SEIM - Security Event and Incident Management
IPS - Intrusion Prevention System	SQL - Structured Query Language
JSON - JavaScript Object Notation	STIG - Service Technical Implementation Guide
LDAP - Lightweight Directory Access Protocol	TACAS - Terminal Access Controller Access System
LUA - Lightweight Programming Language	TCP - Transmission Control Protocol
NICE - National Initiative for Cybersecurity Education	VLAN - Virtual Local Area Network
NIST - National Institute of Standards and Technology	VPN - Virtual Private Network
OSI - Open Systems Interconnection	WPA - WiFi Protected Access
PCAP - file format for Packet Capture	

DACUM Panel

Dr. Gregory Braxton, Newport News Shipbuilding

Kane Crisler, Packet Forensics

Joshua Cox, Towne Bank

Eric Hacecky, Thomas Jefferson National Accelerator Facility

Colleen Lammers, Booz Allen Hamilton

Jim Newman, Peregrine

Richard Severinghaus, CRTN Solutions, LLC

Stephen Watkins, G2 Ops, Inc.

Major Dennis A. Adezas, Joint Forces Staff College

Jennifer Romero, CISSP, AERMOR, LLC

DACUM Facilitator

Jennifer Stevens, Chief Operating Officer
Virginia Advanced Study Strategies

DACUM Research Chart

Cybersecurity Analyst



Produced by:



DACUM Job Analysis Research Chart for **Cybersecurity Analyst**

----- Duties -----	----- Tasks -----										
A Assess Cyber Risks	A.01 Identify info system assets	A.02 Identify security vulnerabilities	A.03 Identify attack vectors	A.04 Quantify business value of assets	A.05 Brief stakeholders *	A.06 Review policies and procedures	A.07 Test response processes	A.08 Create virtual test environments			
B Protect Information Assets	B.01 Create protection plan	B.02 Create contingency plan	B.03 Create disaster recovery plan	B.04 Provision user accounts	B.05 Implement access controls (i.e. black lists, white lists, geofence)	B.06 Install network devices (i.e. IDS, IPS, firewall, web filter)	B.07 Configure network devices (i.e. IDS, IPS, firewall, web filter)	B.08 Install host-based security systems (i.e. antivirs, malware, sensors)	B.09 Configure host-based security systems (i.e. anti-virus, malware, sensors)	B.10 Create investigative and configuration scripts	B.11 Ensure data encryption (i.e. data at rest, data in transit removeable media)
	B.12 Ensure physical security controls	B.13 Ensure environmental controls	B.14 Recommend security requirements	B.15 Manage wireless access points	B.16 Create network diagrams	B.17 Maintain network diagrams	B.18 Create penetration test plans	B.19 Request ASI	B.20 Backup critical data	B.21 Manage network device life-cycles	B.22
C Detect Cybersecurity Events	C.01 Monitor network devices	C.02 Analyze output of network devices	C.03 Analyze threat feeds	C.04 Monitor wireless access points	C.05 Review network diagrams	C.06 Set audit flags	C.07 Analyze external data (i.e. darknet, passive DNS, BGP)	C.08 Document historical findings	C.09 Maintain historical Packet Capture (PCAP)	C.10 Analyze audit logs	C.11 Analyze vulnerability scans
	C.12 Hunt potential threats in network traffic	C.13 Conduct organizational penetration tests	C.14 Generate penetration test documentation	C.15 Challenge personnel need-to-know/authorizations							
D React to Cybersecurity Events	D.01 Initiate response procedures	D.02 Assess security event	D.03 Report event to supervisor *	D.04 Determine escalation	D.05 Communicate with stakeholders *	D.06 Maintain stakeholder call list	D.07 Contain security incident	D.08 Trace source of threat	D.09 Preserve evidence of event	D.10 Document steps taken	D.11 Estimate damage of security incident
	D.12 Sever network activity	D.13 Report estimated time of restoration	D.14 Document evidentiary process								
E Restore Secure Environment	E.01 Determine scope of restoration	E.02 Create restoration plan	E.03 Coordinate restoration efforts	E.04 Rebuild info system	E.05 Reimage information system	E.06 Restore critical data	E.07 Test restored environment	E.08 Validate restored environment	E.09 Document lessons learned	E.10 Document recovery processes	
F Increase Security Awareness	F.01 Create security awareness materials	F.02 Create acceptable use policies	F.03 Participate in security exercises	F.04 Distribute security info to users	F.05 Conduct cybersecurity training	F.06 Conduct phishing campaign	F.07 Reverse engineer malware	F.08 Conduct security awareness assessment	F.09 Report assessment results	F.10 Recommend procedures to correct security issues	
G Maintain Professional Knowledge	G.01 Complete cybersecurity training	G.02 Maintain industry certifications	G.03 Read technical literature (i.e. books, blogs, articles, etc.)	G.04 Attend professional conferences	G.05 Maintain operating environment qualifications	G.06 Practice through trial and error	G.07 Maintain professional memberships				

* Denotes a recurring task