Cybersecurity

Employer Signaling System by the Greater Washington Partnership

Generated: April 8, 2026

IT Fundamentals

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Recognize the importance that cybersecurity plays in managing information and systems, and demonstrate an understanding of the way systems are vulnerable and can be manipulated.	knowledge	3
b	Install and maintain operating systems (OSs) (computer and mobile)	ability	3
c	Understand how to manage sytems at an entyerprise level	knowledge	2
d	Install, patch, and configure software in an enterprise environment including designating access rights	ability	3
e	Install, upgrade, and configure hardware in an enterprise environment including technologies used to collect, analze, record, and share information in business operations	ability	3
f	Explain and describe data encoding basics	knowledge	2
g	Identify and describe basic file types and demonstrate fundamental file management	skill	2
h	Apply networking fundamentals to infrastructure systems	skill	3
i	Identify trending technologies such as AI, machine learning, and quantum computing, their fundamental architecture, and the impact on cybersecurity	knowledge	2
j	Explain the fundamentals of delivering information and applications using web architecture.	knowledge	2

Networking Fundamentals

Label	KSAC Description	KSA	Bloom's Taxonomy Level
b	Understand the OSI model, identify the layers and how they applies to an example network	knowledge	2
f	Configure Understand IPv4 subnets.	skill knowledge	1
g	Compare public IP addresses and private IP addresses.	knowledge	2
i	Interpret classless network ID (CIDR block notation).	knowledge	2
j	Explain IPv6	knowledge	2
l	Explain domain naming conventions (UNC path, FQDN, host name).	knowledge	3
m	Explain how DNS works.	knowledge	2
n	Compare Network Address Translation and Port Address Translation (NAT vs PAT).	knowledge	2
o	Draw a network diagram.	skill	3
p	Analyze the output from networking utilities (e.g. Netstat, Tracert, Traceroute, Ping, IPConfig, IFConfig).	ability	3
q	Discuss network software integration (client software (e.g. Windows 10 or Ubuntu) and server software).	ability	3
r	Discuss network hardware integration (workstations, desktop, mobile devices).	knowledge	2
s	Communicate best practices for troubleshooting networking issues.	knowledge	3
t	Understand the purpose and basic operations of virtual private networks (VPNs)	knowledge	1
u	Understand Dynamic Host Configuration Protocol (DHCP)	knowledge	1

Programming/Scripting Fundamentals

Label	KSAC Description	KSA	Bloom's Taxonomy Level

a	Understand basic programming constructs and demonstrate fundamental programming skills including the use of variables, loops, conditional branching, and functions.	skill	3
b	Design, implement, test, and debug a program that uses each of the following fundamental programming constructs: basic computation, simple I/O, standard conditional and iterative structures.	skill	3
c	Write a program that uses file I/O to provide persistence across multiple executions.	skill	2
e	Understand and apply basic scripting including writing and executing an automation script in Poweshell and/or Linux using constructs such as branching and loopoing	skill	3
f	Write programs that use each of the following data structures: arrays, records/structs, strings, linked lists, stacks, queues, sets, and maps.	skill	3
g	Understand the use of version control systems (e.g. Git) in code management.	knowledge	1

Cloud Fundamentals

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Describe the fundamental cloud components (e.g., shared or dedicated processing, storage, memory, networking, hypervisor).	knowledge	2
b	Differentiate between public, private, and hybrid clouds (i.e. deployment models).	knowledge	2
c	Describe the shared responsbility model for mainatining secure cloud systems	knowledge	2
d	Demonstrate an understanding of cloud architecture and the capabilities of services such as AWS, Azure, IBM, Oracle and Google.	knowledge	2
e	Instantiate a small computing environment in a cloud service.	ability	3
f	Identify common breaches and threats in the cloud environment.	knowledge	1

Label	KSAC Description	KSA	Bloom's Taxonomy Level
g	Understand how to set security configurations in a cloud environment.	knowledge	2
h	Understand a variety of cloud services and what problems each is meant to solve (e.g. Infrastructure as a serice (IaaS, Platform as a service (PaaS), or Function as a Service (FaaS) / Serverless).	knowledge	2

Cybersecurity Basics

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Examine and employ principles of cybersecurity including its goals, objectives, and purposes	ability	2
b	Describe the need for security and identify security risks and ssociated security safeguards and methodologies (e.g., auditing).	knowledge	2
c	Explain the need for confidentiality, integrity, and availability (CIA) and identify types of controls (e.g., deterrent, preventative, detective, compensating, technical and administrative)	knowledge	1
d	Explain security in terms of authentication, authorization, and accounting (AAA) as well as access	knowledge	3
e	Understand the purpose and function of cybersecurity technology so identifying and implementing the various tools necessary to improve an organization's resiliency and reduce the possibility of data breaches	ability	3
f	Describe, recognize, and mitigate major security threats (e.g., adware, viruses, spyware, trojans, rootkits, logic bombs, worms, spyware, ransomware, spoofing, hacking, phishing, and ploymorphic polymorphic malware), using the tools standard in the industry	skill	4
g	Describe the components of the physical environment (e.g., wiring closets, server rooms, data centers) and physical security systems.	knowledge	2
h	Describe the need for security in networking (e.g., firewalls, access controls, encryption, demilitarized zone).	knowledge	2

Label	KSAC Description	KSA	Bloom's Taxonomy Level
i	Understand the indicators of compromise (IOCs) and their use in determining whether an attack has happened or is in progress	knowledge	3
j	Track and catalog computing assets through inventory management, devices and software	ability	2
k	Describe the need for security in application development.	knowledge	2
l	Describe computer forensic techniques, their importance in incident response, and their relevance to law enforcement	knowledge	2
m	Recognize and describe industry threat models (CVE, CWE, threat intel feed, etc).	skill	2
n	Demonstrate and recognize common cyber-attack techniques such as the cyber kill chain and the MiTRE ATT&CK framework	knowledge	3
o	Describe attackers (black hat, white hat, nation states, etc.) and techniques (cybercriminals, APTs).	knowledge	2
p	Describe and understand social engineering attacks (e.g., shoulder surfing, dumpster diving, tailgating, impersonation, hoaxes, phishing, spear phishing, whaling, vishing),	knowledge	2
q	Understand the issues with passwords and the tools and techniques available to crack passwords (e.g. brute force, dictionary attacks, birthday attacks, rainbow attacks and other hybrid attacks).	knowledge	2
r	Desctribe and discover vulnerabilities, understanding concepts and tools of vulnerability assessment, scanning, and penetration testing, and the work of red .purple and blue teams.	knowledge	2
s	Demonstrate an understanding of adversarial thinking using capture the flag (CTF) and other techniques.	skill	3
t	Understand the concept of digital trust computing and the Zero Trust principles	knowledge	2
u	Describe cyber threat intelligence (CTI) and its role in cybersecurity	knowledge	2

Label	KSAC Description	KSA	Bloom's Taxonomy Level
v	Recognize that an enterprise security requires a holistics strategy that considers people, process, and technology.	knowledge	2
w	Categorize system contrils in compliance with government and industry standards including NIST Cybersecurity Framework, FISMA, FEDRAMP, PCI/DSS, HIPAA (as relevant depending on industry), and ISO standards	knowledge	4

Privacy Ethical, Legal and Regulatory Considerations

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Describe how global legal, ethical, and regulatory constraints might impact cybersecurity.	knowledge	2
b	Identify the established legal, ethical and regulatory issues in cybersecurity facing organizations.	knowledge	2
c	Explain how ethical, legal, and regulatory issues should/must be considered in securing systems and data.	knowledge	2
d	Understand the limitations of cybersecurity.	knowledge	2
f	Identify the established privacy issues in cybersecurity facing organizations including sensitive information	knowledge	2
g	Explain how privacy must be considered in securing systems and data.	knowledge	2
i	Demonstrate awareness of personal privacy and how cybersecurity can protect it	knowledge	3
j	Describe the tradeoffs between privacy and security.	knowledge	2
k	Identify the need for personal security in today's digital ecosystem and describe how personal identification, including personally idetifiabe information (PII) and person health information (PHI), can be safeguarded	knowledge	2

Incident Response

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Understand the concept of a Cybersecurity Operations Center (CSOC).and how network security is implemented in the CSOC	knowledge	2
b	Understand log filtering and aggregation.	knowledge	2
c	Understand SIEM technology.	knowledge	2
d	Understand the role of alert signatures.	knowledge	2
e	Run queries on event data.	ability	3
f	Understand forensics and chain of custody.	knowledge	2
i	Apply Incident Response procedures (e.g. preparation, incident identification, escalation and notification, mitigation steps, lessons learned, reporting, recovery procedures, first responder, incident isolation, quarantine, device removal, and data breach).	skill	3
j	Construct a timeline of a cybersecurity incident.	ability	3
k	Implement a recovery procedure.	skill	3
l	Conduct periodic cybersecurity training exercises.	skill	3
m	Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, camera vs. guard).	knowledge	4
n	Create, edit and use roles and system management tools.	ability	3
o	Implement Access Control Lists (ACL).	skill	3
p	Deploy a server hardening plan.	skill	3
q	Implement a Network Access Control (NAC) plan.	skill	3
r	Interpret alarms and alert trends.	skill	2
s	Differentiate between types of enetration testing (e.g., Black box, White box, Gray box).	knowledge	4

Network Security & Engineering

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Apply networking fundamentals to infrastructure in an organization including Defense in Depth	skill	3
b	Select network storage interfaces (e.g., fiber channel, Internet Small Computer System Interface [iSCSI], Fiber Channel over Ethernet [FCoE], Serial Attached SCSI [SAS], Network File Systems [NFS], Network Attached Storage/Server Message Blocks [NAS/SMB]).	skill	3
c	Setup and maintain secure roles and system management techniques (e.g., password, group, and user privilege policies and monitoring).	skill	4
d	Demonstrate an understanding of network security devices (IDS, IPS, FW, NGFW, WAF, CDN, etc.).	kowledge	3
e	Design a secure small office/home office (SOHO) network	skill	3
f	Apply network protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP, etc.) and their impact on security	skill	3
g	Apply Ipv4 and IPv6 securely	skill	2
h	Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, antenna placement, power level controls).	skill	2
i	Apply the principles of secure network design (e.g., DMZ, subnetting, NAT/PAT, remote access, telephony, virtualization, honeypots).	skill	3
j	Implement port security, including an undersanding of port scanning and network traffic monitoring	skill	2
k	Understand how to mitigate network threats (e.g., flood guards, loop protection, implicit deny, network separation, log analysis, Unified Threat Management, peripheral and removable media).	knowledge	2
l	Describe the characteristics and uses of networks, network devices, and components	knowledge	2
m	Design a basic network diagram given a specific need and set of hosts.	skill	3

Label	KSAC Description	KSA	Bloom's Taxonomy Level
n	Install and configure network security mechanisms (firewalls, switches, load balancers, proxies, security gateways, spam filters, IDS/IPS, VPN, etc.).	skill	3
o	Understand and use basic network assessment tools (e.g. Wireshark, NMAP, port scanner)	knowledge	3
p	Understand, setup, and maintain the key cybersecurity principles in network defense (defense in depth, minimizing exposure, etc.).	skill	4
q	Understand the process of vulnerability identification and assessment.	knowledge	2
r	Understand, setup and maintain user roles and system management techniques (e.g., password, groups, user privilege policies and monitoring).	knowledge	2
s	Monitor and manage a network using Unified Threat Management (UTM)	skill	3
t	Manage PKI and certificates (transport encryption, non-repudiation, hashing, digital signatures).	skill	2
u	Understand the concept of opening/extending the network perimeter and the role of a cloud access security broker (CASB).	knowledge	2
v	Identify threats using discovery tools and utilities (e.g., protocol analyzer, vulnerability scanner, honeypots, honeynets, port scanner).	ability	3

Systems Security

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Explain the objectives and functions of modern operating systems, identify potential threats to operating systems and list the security features designed to guard against them.	knowledge	2
b	Discuss networked, client-server, distributed operating systems and how they differ from single user operating systems.	knowledge	2

Label	KSAC Description	KSA	Bloom's Taxonomy Level
c	Understand the role and importance of physical security, including proximity securiity (proximity readers, access lists, biometrics, and protected distribution.	knowledge	2
d	Perform authentication control	skill	3
e	Imolement a life cycle methodology including continuous monitoring and end of life managemnt	skill	3
f	Use the kernel and user mode for executing progams in an operating system.	skill	4
g	Describe the need and the potential run-time problems arising from the concurrent operation of separate tasks.	knowledge	2
h	Summarize techniques for achieving synchronization in an operating system (e.g., describe how to implement a semaphore using OS primitives).	knowledge	4
i	Describe the difference between processes and threads.	knowledge	2
j	Summarize the principles of virtual memory as applied to caching and paging.	knowledge	4
k	Describe the role of identify and access management to manage who can access what in an neterprise	knowledge	
l	Implement authorization control (e.g., least privilege, separation of duties, mandatory access, rule-based access control, role-based access control), so managing priveleged access	skill	3
m	Understand authentication techniques (e.g., tokens, common access card, smart card, multifactor authentication (MFA), single sign-on (SSO), biometrics, personal identification verification card, username, federation, transitive trust/authentication).	knowledge	2
n	Understand security implications of third party connectivity and access.	knowledge	2
o	Discuss hypervisors and the need for them.	knowledge	2
p	Create, configure, and use virtual machines.	skill	3

Data Security

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext to ciphertext.	knowledge	2
b	Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.	knowledge	2
c	Implement end-to-end data security including maintaining data security using data labeling, handling and disposal, as required by policy	skill	3
d	Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics.	knowledge	2
e	Compare and contrast a variety of forensics tools.	knowledge	4
f	Use the concepts of authentication, authorization, access control, and data integrity.	skill	2
g	Implement secure storage of passwords and PII.	skill	3
h	Understand the various techniques for data backup and data erasure.	knowledge	2

Secure Software

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Choose the appropriate data structure for modeling a given problem.	skill	3
b	Implement a divide-and-conquer algorithm for solving a problem.	skill	3
c	Implement a coherent abstract data type, with loose coupling between components and behaviors.	skill	3
d	Identify common coding errors that lead to insecure programs (e.g., buffer overflows, memory leaks, malicious code).	knowledge	3
e	Apply the principles of least privilege, defensive programming, and fail-safe defaults.	ability	3

Label	KSAC Description	KSA	Bloom's Taxonomy Level
f	Write code with logging capabilities.	skill	2
g	Integrate security in all phases of the software development life cycle (SecDevOps).	ability	3
h	Understand web applicatin issues using OWASP	knowledge	2
i	Understand basics of securing web apps - SQL Injection and other input validation.	knowledge	2
j	Understand software bill of materials (SBOM).	knowledge	2

Risk Management & Risk Assessment

Label	KSAC Description	KSA	Bloom's Taxonomy Level
a	Understand the basic principles of risk and describe risk management role in the organization (e.g., business continuity concepts, business impact analysis, Identification of critical systems and components, removing single points of failure).	knowledge	2
b	Describe and plan fault tolerance (e.g., hardware replication, RAID, clustering, load balancing, disaster recovery concepts, backup plans/policies, backup execution/frequency).	skill	3
c	Describe the concepts of risk assessment (e.g., disaster recovery plan, IT contingency planning - succession planning,redundancy).	knowledge	2
d	Apply risk assessment techniques to identify, assess, and prioritize risk factors for information assets concepts related to threat vectors and probability/threat likelihood	skill	3
e	Identify concepts of risk calculation (likelihood, ALE, impact, SLE, ARO, MTTR, MTTF, MTBF).	knowledge	2
f	Describe popular methodologies used in industry to manage risk. Including Governance, Risk ancn Compliance (GRC) processes	knowledge	2
g	Describe cybersecurity risk in relation to business risk	knowledge	2

Label	KSAC Description	KSA	Bloom's Taxonomy Level
h	Describe the risk management process for buildng systems and software applications, including connnected systems, thrd-parties, and the supply chain with the concept of due diligence	knowledge	2
i	Explain how cybersecurity incidents affect a business continuity plan.	knowledge	2
j	Identify compliance with regulations and guidelines and how it varies from government to different industries (e.g., healthcare)	knowledge	2
k	Apply cerification and accreditation processes	skill	4
l	Apply audit and compliance processes	skill	5