Writing Cybersecurity Job Descriptions for the Greatest Impact

Keith T. Hall

U.S. Department of Homeland Security

Welcome

Writing Cybersecurity Job Descriptions for the Greatest Impact

Disclaimers and Caveats

- **Content Not Officially Adopted**. The content of this briefing is mine personally and does not reflect any position or policy of the United States Government (USG) or of the Department of Homeland Security.

- **Note on Terminology**. Will use USG terminology in this brief (but generally translatable towards Private Sector equivalents)

- **Job Description Usage**. For the purposes of this presentation only, the Job Description for the Position Description (PD) is used synonymously with the Job Opportunity Announcement (JOA). Although there are potential differences, it is not material to the concepts presented today.

Key Definitions and Concepts (1 of 2)

- *What do you want the person to do?*
  - **Major Duties and Responsibilities**. *"A statement of the important, regular, and recurring duties and responsibilities assigned to the position"* SOURCE: https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/classifierhandbook.pdf
  - **Major vs. Minor Duties**. *"Major duties are those that represent the primary reason for the position's existence, and which govern the qualification requirements. Typically, they occupy most of the employee's time. Minor duties generally occupy a small portion of time, are not the primary purpose for which the position was established, and do not determine qualification requirements"* SOURCE: https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/positionclassificationintro.pdf
  - **Tasks**. *"Activities an employee performs on a regular basis in order to carry out the functions of the job."* SOURCE: https://www.opm.gov/policy-data-oversight/assessment-and-selection/job-analysis/job_analysis_presentation.pdf

Key Definitions and Concepts (2 of 2)

- *What do you want to see on resumes that qualifies them to do this work?*

- **Competency**. *"Competency is a **measurable** pattern of **knowledge, skills, abilities (KSAs), behaviors**, and other characteristics that an individual needs to perform work roles or occupational functions successfully. Competencies specify the 'how' of performing job tasks, or what the person needs to do the job successfully."* SOURCE: https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/ https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/

  - **Behaviors** – *"the way in which one acts or conducts oneself, especially toward others"*
  - **Knowledge** – *"facts, information, and skills acquired by a person through experience or education; the **theoretical or practical** understanding of a subject"*
  - **Abilities** – *"**possession** of the means or skill **to do something**"*
  - **Skills** – *"the ability to do something **well; expertise**"*

Where to start?

Why Start Here?

- ***"What's the problem? – I'll just put out my old announcement until I get the right candidate.."***
  - Did the position require a skill not listed on the announcement?
  - How much end-to-end time or resources will be wasted running through the responses?

- ***"I don't have to hire anyone, I just need to outsource the work.."***
  - Don't you still need to articulate your requirements into the contract?
  - Is this a Mission Critical Function (MCF) or Inherently Governmental Function (IGF)? If so, should it be outsourced?

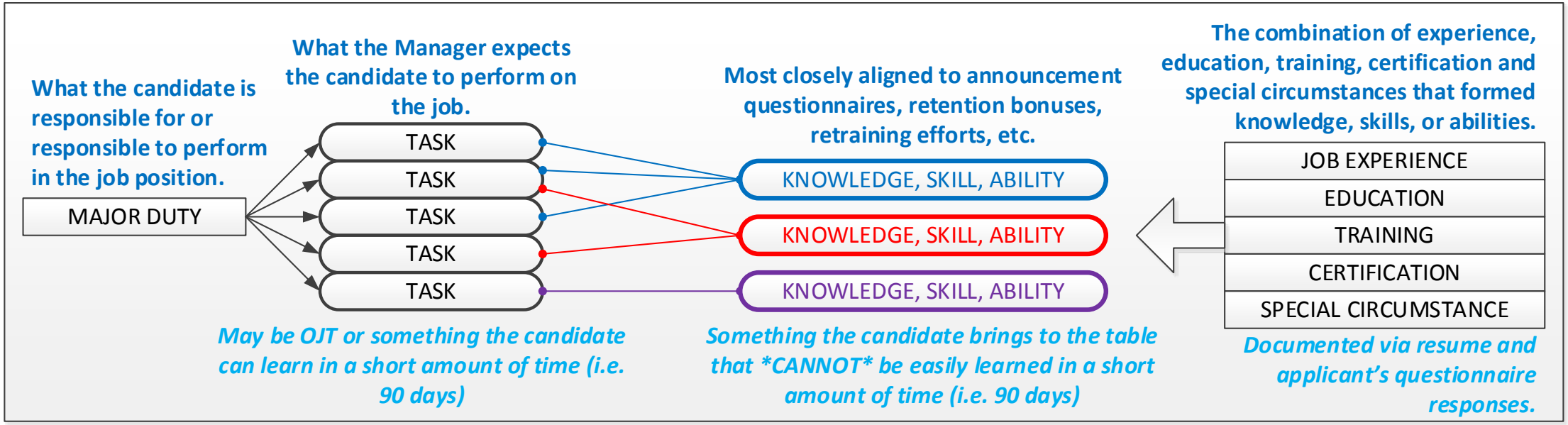
- ***"I keep reading about the cyberskills gap, but I don't see how it's any different from non-cyber positions?"***
  - True, the Intelligence and Acquisition fields fall into very similar skill gap patterns due to high demand and shifting underlying requirements. However, cybersecurity technical transition cycles are overall either faster or have greater permutations possible.
  - It seems easy, but it's not..

Why is a Job Description So Important?

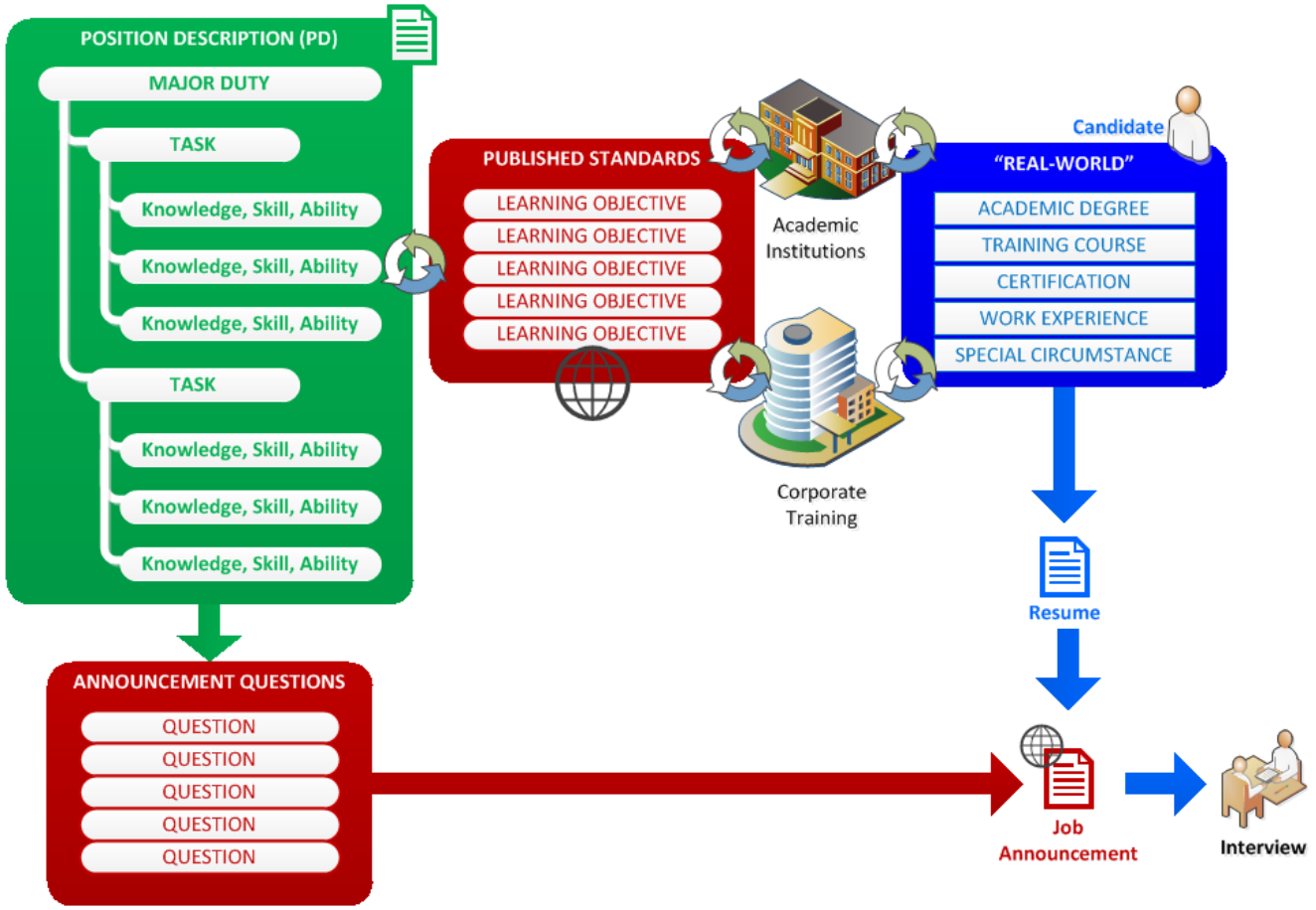
- **Tactical Reason** : *"I meant what I said and I said what I meant."* SOURCE: Dr. Seuss, Horton Hatches and Egg, Random House, 1940
  - Accuracy in the Job Opportunity Announcement (JOA)
  - Clearly communicates intent ***directly*** to Job Candidates
  - Overall better Job Candidate quality in response

- **Strategic Reason** : Proactive Workforce Planning
  - Can future plans be supported with ***existing*** skillsets?
  - What new skillsets are required?
  - What is the current gap in delivery capability that re-training current workforce cannot achieve in sufficient time or in quantity?

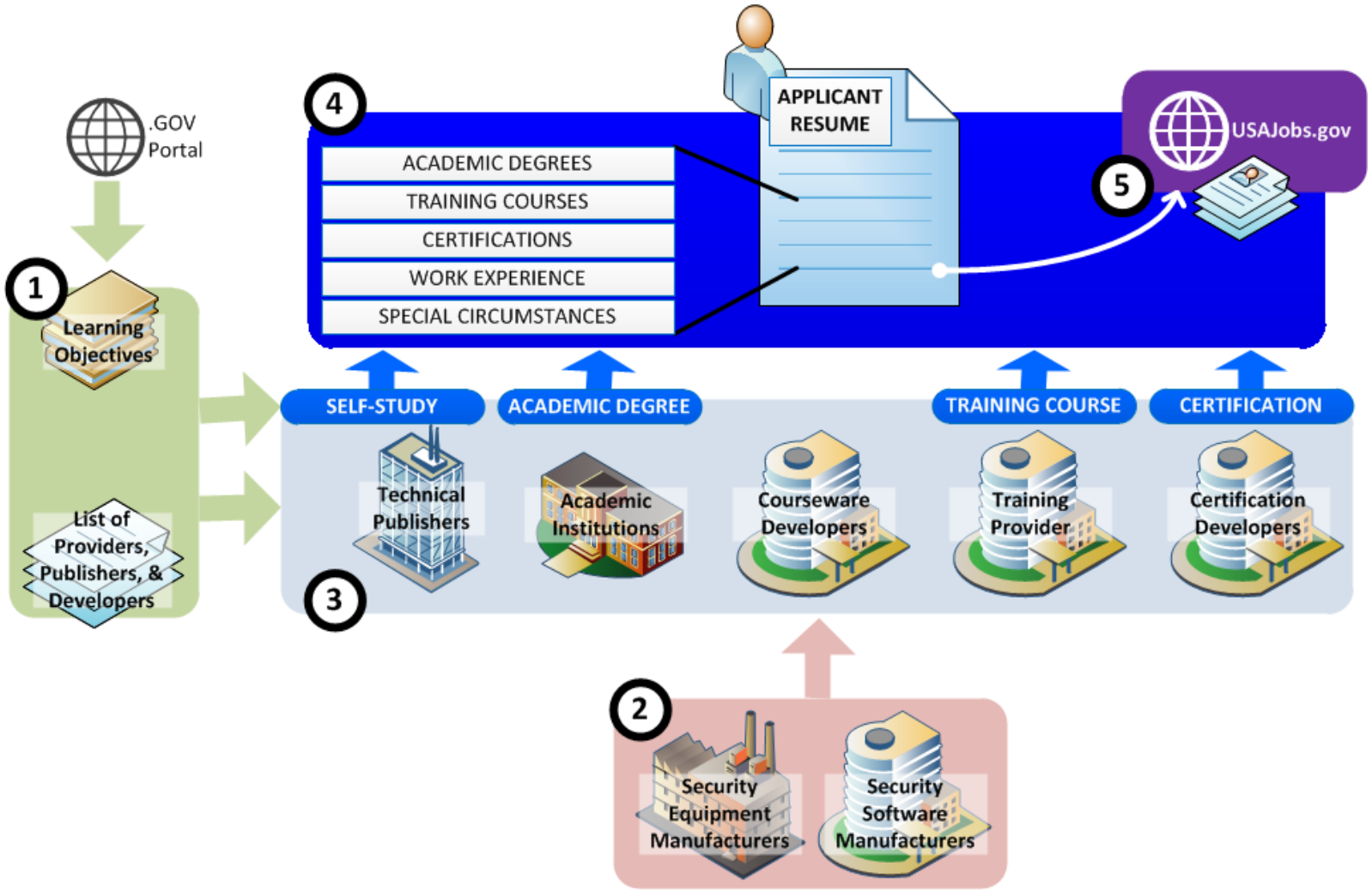
About Job Description Alignment (Tactical Example)



About the Dynamics of Hiring



The Experience, Education, Training and Certification Ecosystem



Cyber Positions, Skillset Attributes & Elements (Some Examples)

- **Offensive vs Defensive**. Ex. Penetration Tester vs. Public Key Infrastructure (PKI) Specialist.
- **Proactive, Continuous, vs Reactive**. Ex. Security Engineer vs. Incident Responder.
- **Hands-On vs Non-Hands-On**. Ex. Operations vs. Analysis.
- **Proficiency Level**. Ex. Basic, Journeyman, Advanced.
- **Technology Focus**. Ex. Critical Infrastructure Protection (CIP), Anti-Malware, Security-Related Technology, Non-Technology Based (ex. Administration, Support, Training, Cyber-Related Complimentary Security Area).
- **OJT (< 90d) vs Pre-Existing (> 90d)**. Ex. Orientation vs. Core Skillset.
- **Specificity Level**. Ex. OPM Mosaic or Category vs. Specialty or Sub-Category (ex. NICE, HSAC, FAI, AT&L, etc) vs. Specific Vendor or Technology

Vendor-Independent vs. Vendor-Specific Experience, Education, Training and Certifications

VENDOR-INDEPENDENT

ADVANTAGES:

- Fewer legal hurdles (Government Competition Standpoint)
- Covers Knowledge and Concepts

DISADVANTAGES:

- Hands-on time-to-operations can be > 90 days

VENDOR-SPECIFIC

ADVANTAGES:

- Hands-on time-to-operations can be < 90 days

DISADVANTAGES:

- Normally narrower in scope (may or may not provide direct applicability to the organization)

Training vs Certification Baselines

TRAINING

- **Entry / Basic-Level** (e.g. Taking the class or "I can learn from the book"; ***knowledge of***)
- **Journeyman / Mid-Level** (e.g. Able to perform or "I can apply the book"; ***skill or ability to***)
- **Mastery or Expert / Senior-Level** (e.g. Teaching the class or "I can teach others the book"; ***expert in*** **or** ***mastery of***)
- **Senior Mastery-Expert / SME-Level** (e.g. authoring new materials or "I can write the book"). Ex. ***Developing new material where no pre-existing material exists***.

CERTIFICATIONS

- **Vendor-Independent or Knowledge-Based Certifications** (represent a ***minimum or baseline level of knowledge***) Analysis functions could be <90d; vendor-specific, ***hands-on functions >90d***
- **Hands-on, Vendor-Specific Certifications** (represent a ***minimum or baseline level of skill or ability***) Vendor-specific, ***hands-on functions <90d***

Specificity Levels

		GRANULARITY	EXAMPLE CONTENT	EXAMPLE USAGE
I	CATEGORY	Broad category	OPM MOSAIC (Cybersecurity)	Background or Foundational Knowledge Requirements; Internships
II	SUBCATEGORY	Workrole, Functional Area, Major Duty	NICE Framework; DoD AT&L; FAI FAC; CIP	Non-hands-on positions; Generalists
III	TYPE	Specific Technologies, Devices or Programming Languages	Vendor-specific certifications, specific programming languages, or technology-specific coursework	Hands-on positions
IV	SUBTYPE	Specific Techniques, Specialties, or Research Areas	Specific techniques or very granular technical skill requirements	Highly Technical Specialists

Case Study: Security Programmer

Level I

CATEGORY-LEVEL COMPETENCIES & KSA's

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- **Computer Languages** - Knowledge of computer languages and their applications to enable a system to perform specific functions.
- **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
- **Information Systems Security Certification** - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.
- **Information Systems/Network Security** - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: https://www.chcoc.gov/content/competency-model-cybersecurity

Further information about OPM MOSAICs are available at https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/mosaic-studies-competencies.pdf and https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/

Case Study: Security Programmer (Continued)

Level II

SUBCATEGORY-LEVEL COMPETENCIES & KSA's

Example ORGANIZED BY MAJOR DUTIES OR WORKROLES

PROACTIVE:

- **Secure Coding** – skills describing someone who develops secure code. Will be specialized in one or more programming languages. This person is a developer.
- **Code Reviewing** - skills describing someone who reviews code for security flaws. Will be specialized in one or more programming languages. This person is NOT a developer, but more along the lines of a Vulnerability Analyst.

CONTINUOUS:

- **Code Validation & Integrity Checking** - skills describing the process of digitally signing code, then validating authenticity throughout the lifecycle (including patching and updating). May not actually be a programmer or understand code at all. Generally may need some knowledge of cryptographic hashes, checksums, operational update processes, etc.

REACTIVE:

- **Malware Analysis** - skills describing someone who can analyze code injected into systems, hardware, software, etc. Generally must have some knowledge of Assembler and at least one other programming language.
- **Forensics Analyst Analysis** - skills describing someone who can harvest malware
- **Law Enforcement Forensics Analysis** - able to testify in court or prepare evidence sufficiently for court about harvested malware.

Case Study: Security Programmer

TYPE-LEVEL COMPETENCIES & KSA's – Ex. SPECIFIC TECHNOLOGY, PROGRAMMING LANGUAGE, DEVICE

Level III

@Formula	Axum	Clean	Draco	FoxBase	IMP	LINC	Miranda	occam	POP-11	SAIL	Swift (parallel scripting Lang)	Wyvern	Powerhouse
A# (Axiom)	Babbage	Clipp[illegible]	D[illegible]ON	FoxPro	Inform	Lingo	ML	occam-p	PortablE	SALSA	SYMPL	X#	Q (equational prog Lang)
A+	BAI[illegible]	CLIS[illegible]	D[illegible]	FP	Io	Linoleum	Moby	Octave	PostScript	SAM76	SyncCharts	X10	Qi
[illegible]	[illegible]	Cloj[illegible]	D[illegible]MO	FPr	Ioke	LIS	Model 204	OmniMark	PowerBuilder - 4GL GUI appl. gen from Sybase	SAS	SystemVerilog	XBL	QPL
[illegible]0 System	[illegible]IC	CLU[illegible]	E[illegible]	Franz Lisp	IPL	LISA	Modelica	Onyx	PowerShell	SASL	TACL	XC (exploits XMOS architecture)	rc
ABAP	bc	CMS EXEC	Ease	F-Script	ISLISP	Lisaac	Modula	Opa	PPL	Sather	TACPOL	XL	Rlab
ABC	BCPL	CMS-2	Easy PL/I	FSProg	ISPF	Lisp - ISO/IEC 13816	Modula-2	Opal	Pro*C	Sawzall	TADS	Xojo	Sed
ABC ALGOL	BeanShell	COBOL - ISO/IEC 1989	Easy prog Lang	Game Maker Lang	ISWIM	Lite-C	Modula-3	OpenCL	Processing	SBL	TAL	XOTcl	Span
ABLE	Bertrand	Cobra	EASYTRIEVE PLUS	GameMonkey Script	J#	Little b	Mohol	OPL	Processing.js	Scala	Tcl	XPL	TeX
ABSET	BETA	CODE	ECMAScript	GAMS	J++	LiveCode	MOO	OPS5	Prograph	Scheme	Tea	XQuery	Trac
ABSYS	Bigwig	CoffeeScript	Edinburgh IMP	GAP	JADE	LiveScript	Mortran	OptimJ	PROIV	Scilab	TECO	XSB	Ubercode
ACC	Bistro	Cola	EGL	G-code	Jako	Logo	Mouse	Orc	Prolog	Scratch	TELCOMP	XSLT - See XPath	Unicon
Accent	BitC	ColdC	Eiffel	GDL	JAL	Logtalk	MPD	ORCA/Modula-2	PROMAL	Script.NET	TEX	Zeno	Unix shell
Ace DASL	BLISS	ColdFusion	Elixir	Genie	Janus	LPC	MSIL - deprecated name for CIL	Oriel	Promela	Seed7	TIE	A# .NET	Vala
ACL2	Blue	COMAL	Elm	GEORGE	Java	LSE	MSL	Orwell	PROSE modeling Lang	Self	Timber	ActionScript	Visual Basic .NET
ACT-III	Boo	COMIT	Emacs Lisp	Gibiane	JavaFX Script	LSL	MUMPS	Oxygene	PROTEL	SenseTalk	TMG, compiler-compiler	AMPL	Visual J++
Action!	Boomerang	Common Int Lang (CIL)	Emerald	GLSL	JavaScript	Lua	Napier88	Oz	ProvideX	SequenceL	Tom	Batch (Windows/Dos)	WATFIV, WATFOR
Ada	Bourne shell (including bash and ksh)	Common Lisp (also known as CL)	Epigram	GM	JCL	Lucid	NATURAL	ParaSail (prog Lang)	Pure	SETL	TOM	Bon	WebQL
Adenine	BPEL	COMPASS	EPL	GNU E	JEAN	Lustre	Neko	PARI/GP	Python	Shift Script	Topspeed	CHILL	Winbatch
Agda	BREW	Component Pascal	Erlang	Go	Join Java	LYaPAS	Nemerle	Pascal - ISO 7185	Q (prog Lang from Kx sys)	SIMPOL	TPU	Combined prog Lang (CPL)	X++
Agilent VEE	C--	Constraint Handling Rules (CHR)	es	Go!	JOSS	Lynx	nesC	Pawn	Qalb	SIMSCRIPT	T-SQL	Datalog	xHarbour
Agora	C Shell	Converge	Escapade	GOAL	JOVIAL	M4	NESL	PCASTL	QtScript	Simula	TTCN	DCL	XPL0
AIMMS	C# - ISO/IEC 23270	Cool	Escher	Gödel	Joy	Machine code	Net.Data	PCF	QuakeC	Simulink	TTM	ELAN	Yorick
Alef	C/AL	Coq	Esterel	GOM (Good Old Mad)	JScript	MAD (Michigan Algorithm Decoder)	NetLogo	PDL	R++	SISAL	Turbo C++	ESPOL	YQL
ALF	C++ - ISO/IEC 14882	Coral 66	Etoys	Goo	JScript .NET	MAD/I	NewLISP	PEARL	Racket	S-Lang	Turing	Fjölnir	Z notation
ALGOL 58	Caché ObjectScript	Corn	Euclid	Google Apps Script	Julia	Magik	NEWP	PeopleCode	RAPID	SLIP	TUTOR	Forth	ZOPL
ALGOL 60	Caml	CorVision	Euler	Gosu	Kaleidoscope	Magma	Newspeak	Perl	Rapira	SMALL	TXL	GJ	ZPL
ALGOL 68	Candle	COWSEL	Euphoria	GOTRAN	Karel	make	NewtonScript	PHP	Ratfiv	Small Basic	TypeScript	Godiva	
ALGOL W	Cayenne	CPL	EusLisp Robot prog Lang	GPSS	Karel++	Maple	NGL	Phrogram	Ratfor	Smalltalk	UCSD Pascal	Hack (prog Lang)	
Alice	CDuce	csh	EXEC 2	GraphTalk	KEE	MAPPER (Unisys/Sperry) now part of BIS	Nial	Pico	REBOL	SML	Umple	Haxe	
Alma-0	Cecil	Csound	Executable UML	GRASS	Kojo	MARK-IV (Sterling/Informatics) now VISION:BUILDER of CA	Nice	Pict	Red	SNOBOL(SPITBOL)	Uniface	Hope	
AmbientTalk	Cel	CSP	F#	Groovy	Kotlin	Mary	Not eXactly C (NXC)	Pike	Redcode	Snowball	UNITY	IBM Basic assembly Lang	
Amiga E	Cesil	CUDA	Factor	HAL/S	KRC	MASM Microsoft Assembly x86	Not Quite C (NQC)	PIKT	REFAL	SOL	UnrealScript	IDL	
AMOS	Ceylon	Curl	Falcon	Hamilton C shell	KRL	Mathematica	NPL	PILOT	Reia	SP/k	VBA	IPTSCRAE	
APL	CFML	Curry	Fancy	Harbour	KRYPTON	MATLAB	NSIS	Pipelines	Revolution	SPARK	VBScript	JASS	
App Inventor for Android's visual block Lang	Cg	Cyclone	Fantom	Hartmann pipelines	ksh	Max (Max Msp - Graphical prog Env)	Nu	PL/0	rex	SPIN	Verilog	Joule	
AppleScript	Ch	Cython	FAUST	Haskell	L# .NET	MaxScript internal Lang 3D Studio Max	NWScript	PL/B	REXX	S-PLUS	VHDL	KIF	
Arc	CHAIN	Dart	Felix	High Level Assembly	LabVIEW	Maya (MEL)	NXT-G	PL/C	RobotC	SPS	Visual Basic	Legoscript	
ARexx	Chapel	DASL (Datapoint's Adv sys Lang)	Ferite	HLSL	Ladder	MDL	Oak	PL/I - ISO 6160	ROOP	Squeak	Visual DataFlex	Lithe	
Argus	Charity	DASL (Distr app Spec Lang)	FFP	Hop	Lagoona	Mercury	Oberon	PL/M	RPG	Squirrel	Visual DialogScript	M2001	
AspectJ	Charm	DataFlex	FL	Hugo	LANSA	Mesa	Obix	PL/P	RPL	SR	Visual Fortran	Maxima (see also Macsyma)	
Assembly Lang	Chef	DATATRIEVE	Flavors	Hume	Lasso	Metacard	OBJ2	PL/SQL	RSL	Stackless Python	Visual FoxPro	MIVA Script	
Ateji PX	CHIP-8	dBase	Flex	HyperTalk	LaTeX	Metafont	Object Lisp	PL-11	RTL/2	Starlogo	Visual J#	NASM	
ATS	chomski	dc	FLOW-MATIC	IBM HAScript	Lava	MetaL	Object Pascal	PL360	Ruby	Stata	Visual Objects	NetRexx	
Autocoder	ChucK	DCL	FOCAL	IBM Informix-4GL	LC-3	Microcode	Object REXX	PLANC	Rust	Stateflow	Visual Prolog	Nickle	
AutoHotkey	CICS	Deesel (formerly G)	FOCUS	IBM RPG	Leda	MicroScript	Objective-C	Plankalkül	S/SL	Strand	VSXu	o:XML	
AutoIt	Cilk	Delphi	FOIL	ICI	LIL	MIIS	Objective-J	Planner	S2	Subtext	Vvvv	Obliq	
AutoLISP / Visual LISP	CL (IBM)	DIBOL	FORMAC	Icon	LilyPond	MillScript	ObjectLOGO	PLEX	S3	SuperCollider	WebDNA	OpenEdge ABL	
Averest	Claire	DinkC	Fortran - ISO/IEC 1539	Id	Limbo	MIMIC	Obol	PLEXIL	SabreTalk	SuperTalk	Windows PowerShell	P#	
AWK	Clarion	Dog	Fortress	Idris	Limnor	Mirah	OCaml	Plus	SA-C	Swift (Apple prog Lang)	Wolfram	Pizza	

Case Study: Security Programmer (Continued)

Level I

CATEGORY-LEVEL COMPETENCIES & KSA's

OPM MOSAIC-Level Example (Multipurpose Occupational Systems Analysis Inventory - Close-Ended)

- **Computer Languages** - Knowledge of computer languages and their applications to enable a system to perform specific functions.
- **Information Assurance** - Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
- **Information Systems Security Certification** - Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements. Includes developing security certification and accreditation plans and procedures, documenting deficiencies, reporting corrective actions, and recommending changes to improve the security of information systems.
- **Information Systems/Network Security** - Knowledge of methods, tools, and procedures, including development of information security plans, to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.

SOURCE: https://www.chcoc.gov/content/competency-model-cybersecurity

Further information about OPM MOSAICs are available at https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/mosaic-studies-competencies.pdf and https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/

Case Study: Security Programmer

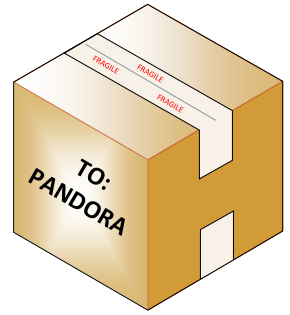
SUBCATEGORY-LEVEL COMPETENCIES & KSA's – Ex. ORGANIZED BY MAJOR DUTIES OR WORKROLES

Level II to III

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	White Team
Acco[illegible] (Forensic)	Computer Engineer	[illegible]ber Intel [illegible]	Electrical Engineer	[illegible]mation Ass[illegible] Architect / Security Architect	Investigator	Management and Program Analyst	Program Manager* / Project Manager*	Senior Information Security Officer or Senior Agency Information Security Officer (SAISO) or Chief Information Security Officer (CISO)*	Teacher Supervisor; if cyber-specific	Workforce Development Specialist; if cyber-specific
Accounti[illegible]icer (Forensic)	[illegible]puter Enginee[illegible]	[illegible]ber Legal [illegible]	Ele[illegible]cs Engineer	[illegible]mation Ass[illegible] Engineer / Security Engineer	Investment Review Board or IT Investment Board (or equivalent)	Manager	Program Manager, Cybersecurity Program Manager, IT Program Manager	Server Administrator	Teacher; if cyber-specific	Workforce Research and Analysis [Variable titling]; if cyber-specific
[illegible]ditor	Comp[illegible]ngineer (E[illegible]ded Systems)	[illegible]ersecurity[illegible]st	Ele[illegible]cs Technician	[illegible]formation[illegible]nce Operational Engineer	IT / Cybersecurity Analyst / Administrator / Manager / Officer	Mathematical Statistician	Programmer	Service Desk Operator	Technical Review Board	
Acquisition Team, Acquisition Initiator	Computer Engineer (Networks)	Cybersecurity Curriculum Developer, Cyber Instructional Curriculum Developer, Cybersecurity Training Manager, Chief Learning Officer (CLO)	Emergency Management Specialist	Information Assurance Specialist; also Information Assurance Manager / Officer	IT / Cybersecurity Program & Project Manager	Mathematician	Programmer Analyst	Service Desk Representative	Technical Support Specialist; Technical Support Personnel	
All Source-Collection Manager	Computer Engineer (Simulations)	Cybersecurity Intelligence Analyst	Engineering Technician (Electrical)	Information Dissemination Manager	IT / Cybersecurity Training, Outreach, and Awareness Professional	Miscellaneous Administration and Program Specialist	Property Disposal Clerk	Signals Intelligence (SIGINT) Exploitation Analyst	Telecommunication Engineer	
All Source-Collection Requirements Manager	Computer Forensic Analyst	Cybersecurity Operations Planner	Enterprise Architect	Information Manager	IT / Cybersecurity Workforce Development/Planning Specialist	Mission / Business Owner	Property Disposal Officer	Site Administrator	Telecommunications Equipment Operator	
All-Source Analyst	Computer Network Defense Analyst / Manager	Cybersecurity Operations Specialist	Enterprise Resource Planner	Information Owner / Steward	IT Auditor	Mission Assessment Specialist	Property Disposal Specialist	Software Architect	Telecommunications Specialist	
Analyst Programmer	Computer Operator	Cyber Policy and Strategy Planner, Cybersecurity Policy & Planning Specialist	Enterprise Risk Manager	Information Resource Manager	IT Capital Planning, Architecture, and Security and Privacy Subcommittees	Multi-Disciplined Language Analyst	Property Disposal Technician	Software Asset Manager	Telecommunications Specialist (Communications Acquisition)	
Application Security Analyst	Computer Programmer	Cybersecurity Research and Forensics Professional	Enterprise Security Architect	Information Security (INFOSEC)	IT Policy and Planning Analyst	Network Administrator	Public Utilities Specialist [Variable titling]	Software Assurance Technician / Engineer	Telecommunications Specialist (Data Transmission)	
Application Security Architect	Computer Scientist	Cybersecurity Training Specialist, Cybersecurity Trainer, Cybersecurity Instructor, Learning Officer, Cyber Instructor, Cyber Professor	Ethical Hacker	Information Security Architect	IT Program Management Specialist	Network Security Analyst	Purchasing Agent	Software Developer	Telecommunications Specialist (Deployment Planning)	
Application Security Engineer	Configuration Management (CM) Manager	Cybersecurity Workforce Manager , Cybersecurity Workforce Specialist	Executive Cyber Leadership (ex. OPM SES, SL, FL, GO) (ex. Director, Chief Information Security Officer, Chief Security Officer, Senior Agency Information Security Officer)	Information Security Auditor	IT Project Management [Parenthetical]	Network Security Engineer	Quality Assurance (QA) / Software Quality Assurance Specialist / Engineer / Test Director*; Release Engineer	Software Engineer	Telecommunications Specialist (Plans & Policy)	
Applications Developer	Content Administrator	Data Administrator	Exploitation Analyst	Information Security Developer, Information Systems Security Developer	IT Program Auditor, IT Security Auditor, IT Auditor	Network Security Officer; also Network Security Specialist	Records and Information Management Specialist	Software Implementer	Telecommunications Specialist (RF Spectrum Management)	
Archivist	Content Staging Specialist	Data Analyst	Financial Administration and Program Specialist	Information Security Specialist	IT Security Project Manager, IT Project Manager, IT Security Program Manager	Network Security Specialist, Network Security Administrator, Network Security Operations Specialist, Network Operations Specialist, Network Analyst, Network Designer, Network Engineer	Red Team	Software Programmer	Telecommunications Specialist (Telecom Management)	
Attorney [Variable titling]	Continuous Diagnostics & Mitigation (CDM) Specialist	Data Architect	Financial Manager	Information System Integrator	IT Specialist	Network Services	Regulatory Affairs Analyst	Software Quality Assurance Specialist	Telecommunications Specialist (Telecom Operations)	
Attorney-Adviser [Variable titling]	Continuous Monitoring Executer	Data Management; also Data Management Systems Security; Data Manager	Financial Specialist	Information System Owner or System Owner	IT Specialist (Applications Software)	Network Systems and Data Communications Analyst	Requirements Analyst / Engineer / Planner; Systems Requirements Planner	Software Specialist	Telecommunications Specialist (Telecom Requirements)	
Auditor [Financial]	Contract Administrator	Data Modeler	Foreign Law Specialist [Variable titling]	Information System Security Engineer	IT Specialist (Customer Support)	Operating Unit/Bureau Executive Management	Research and Development (R&D) Specialist / Engineer	Solutions Architect	Telecommunications Specialist (Test & Evaluation)	
Authorizing Official (AO) or Certifying Official	Contract Negotiator	Data Protection Officer	Forensic Analyst (for Law Enforcement (LE) / Counterintelligence (CI), Advanced)	Information Systems Security Analyst; also Systems Security Analyst; Information Security Analyst	IT Specialist (Data Management)	Operations Personnel / Management; System Operations Personnel	Reverse Engineer	Source Code Auditor	Telecommunications Specialist (Traffic Analysis)	
Authorizing Official/Designating Representative	Contract Price/Cost Analyst	Data Security Analyst, Database Security Analyst, Data Security Officer, Chief Data Security Officer, Chief Data Officer, Data Analyst	Forensic Analyst (non-LE/CI)	Information Systems Security Manager (ISSM)	IT Specialist (Enterprise Architecture)	Operations Research Analyst	Risk / Vulnerability Specialist / Manager	Spectrum Manager	Testing and Evaluation Specialist; Security Test & Evaluation Specialist, Security Test Engineer, Test Engineer	
Blue Team	Contract Specialist	Data Storage Specialist	Freedom of Information Act (FOIA) Official	Information Systems Security Officer (ISSO)	IT Specialist (Internet)	Paralegal Specialist	Risk Assessment Engineers	Staff Accountant	Threat Analyst	
Budget Analyst	Contract Termination Specialist	Data Warehouse Specialist	General Attorney	Information Systems Security Specialist	IT Specialist (Network Services)	Partner Integration Planner	Risk Assessor	Strategic Planning, Policy, and Compliance Professional	Threat Analyst / Counterintelligence Analyst	
Business Analyst	Contracting Officer (CO)	Database Administrator, Database Security Administrator	General Education and Training [Variable titling]; if cyber-specific	Information Technology Architect	IT Specialist (Operating Systems)	Penetration Tester	Risk Executive (Function)	Supply Management Officer	Training Administrator	
Business Intelligence Manager	Contracting Officer (CO), Contracting Officer's Representative (COR), Contracting Officer's Technical Representative (COTR), IT Investment/Portfolio Manager	Database Developer	General Inspection, Investigation, Enforcement, and Compliance Specialist	Insider Threat Program Manager	IT Specialist (Policy and Planning)	Penetration Tester (Application)	Secure Coder and Code Reviewer; Secure Software Engineer	Supply Management Specialist	Training Developer or Instructional Design Specialists	
Cabling Technician	Converged Network Engineer	Database Engineer	General Mathematician and Statistician	Inspector / Investigator	IT Specialist (Security)	Penetration Tester (System and Network)	Secure Software Assessor	Supply Systems Analyst	Training Instructor	
Certification Agent	Cost Accountant	Designated Accrediting Authority (DAA)	General Supply Specialist; if cyber-specific	Inspector General	IT Specialist (Systems Administration)	Platform Specialist	Security Administrator; Server Administrator	System / Application Security Tester	Training Specialist	
Chief Enterprise Architect	CounterIntelligence Analyst	Desired State Manager and Authorizer (DSM)	General Telecommunications [Variable titling]	Instructional Systems Specialist; if cyber-specific	IT Specialist (Systems Analysis)	Portfolio Manger	Security Architect	System Accountant	Training Technician	
Chief Financial Officer (CFO)	Criminal Investigator'	Desktop Support	Governance Manager	Integration Engineer	Keying Material Manager	Principal Security Architect	Security Awareness Training Manager	System Architect or IT Architect*	UNIX/Windows Systems Administrator	
Chief Information Officer (CIO)*	Cryptanalyst	Device Manager (DM)	Government Information Specialist	Intelligence Analyst	Knowledge Manager	Privacy Officer, Chief Privacy Officer	Security Control Assessor	System Evaluator	Vocational Development Specialist; if cyber-specific	
Chief Information Security Officer (CISO)	Cryptographer	Directory Services Administrator	Guidance Counselor	Intelligence Operations Specialist	LAN/WAN Administrator	Privacy Compliance Manager, Privacy Specialist, Privacy Lead	Security Engineer / Architect (for Building-In Security)	System Security Analyst, Systems Analyst	Vocational Rehabilitation Specialist; if cyber-specific	
Claims Assistant / Claims Examiner	Customer Support	Disaster Recovery / Business Continuity Officer [Emergency Administrative Specialist, Physical Security Specialist; Emergency Management Specialist (Preparedness) ; Information Management Specialist]	Head of Agency or Organization (Chief Executive Officer)	Intelligence Planner	Legal Advisor/Contract Attorney	Procurement Analyst	Security Engineer-Operations	Systems Administration; Systems Administrator; also System Administrator, System Security Administrator, Application Security Administrator, Application Administrator, Web Administrator	Vulnerability Assessment Analyst	
Cloud Engineer	Customer Support Specialist	Document Steward	Help Desk, Help Desk Representative, Customer Support, Technical Support Specialist	Intelligence Research Analyst	Legal Assistant	Procurement Clerk	Security Monitoring and Event Analysis	Systems Developer	Warning Analyst	
Cloud Solutions Architect	Cyber Crime Investigator	Education Program Administrator; if cyber-specific	Human Resources Specialist (Information Systems)	Intelligence Specialist	Legal Instruments Examiner	Procurement Technician	Security Solutions Architect	Systems Engineer; Support Engineer	Web Developer	
Common Control Provider	Cyber Defense Analyst	Education Program Specialist; if cyber-specific	Identity Access Manager	Internet	Maintenance Specialist; also Maintenance Engineer	Product Owner	Security Specialist	Systems Programmer	Web Manager	
Communications Security (COMSEC) Manager	Cyber Defense Forensics Analyst	Education Research Analyst; if cyber-specific	Incident responder in-depth	Internet Architect	Malware Analyst	Product Support Manager	Security Specialist (ADP)	Systems Software Engineer	Web Operations Specialist	
Compliance Analyst / Officer / Manager	Cyber Defense Incident Responder	Education Services Specialist; if cyber-specific	Independent Verifier / Validator	Internet Developer	Management Analysis Officer	Program Analysis Officer	Security Specialist (Crypto)	Systems Software Programmer	Webmaster	
Compliance Inspection and Support Specialist	Cyber Defense Infrastructure Support Specialist	Educational Aid [GS-4 and below]; if cyber-specific	Industrial Engineering Technician	Internet Specialist	Management Analyst	Program Analyst	Senior Agency Officials	Target Developer	Website Web Administrator	

DHS PushButtonPD™ NICE Framework Demonstration

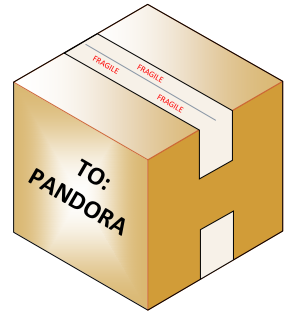
Filtering the Pandora's Box



- **What is a good Task to include?**
  - If the employee does not do it, will you go to HR about it?
  - Is it reasonable that a single person can do all the tasks?
  - Does this (unintentionally) overlap or duplicate with tasks performed by others?
  - Is it well-defined and accurately reflect the Major Duties (vs vague and generic)?

- **What is a good Competency or KSA to include?**
  - Is it a ***need*** (not a ***want***)?
  - Is it ***measurable***? Is it (in some form or another) on their resume or can you interview / test on it – not (a) something you will on-the-job train them later to do; or (b) too vague and opinionated?
  - Are there equivalent or suitable alternatives that are just as good (***or*** versus ***and***)?

Continuing to Filter the Pandora's Box



"Special Qualification Requirements - a statement of any valid knowledge, skill, education, certification, etc., required by the position if it is not readily apparent from reading the description, such as level of typing skill, foreign language proficiency, or licensure." SOURCE: https://www.opm.gov/policy-data-oversight/classification-qualifications/classifying-general-schedule-positions/classifierhandbook.pdf

- **What is a good Competency or KSA to use as a Special Qualification or a Selective Placement Factor?**
  - Is it sufficiently defined to easily pick it out when resume screening? If not, are you able to test it in an interview or phone screen?
  - Do you want to eliminate and screen out candidates without it on their resume? (e.g. a minimum threshold to achieve)
  - Is it truly special (versus commonplace)?

PushButtonPD™

Live Demo

DHS PushButtonPD™ NICE Framework Demonstration

Questions

Writing Cybersecurity Job Descriptions for the Greatest Impact

Helpful Resources

NIST NICE, NICE@nist.gov, https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity

DHS NPPD NICCS Website (Workforce Development page), https://niccs.us-cert.gov/workforce-development, NICCS@hq.dhs.gov

The NICCS Training Catalog – more than 3,000 cybersecurity courses (including certification prep courses) already aligned to the NICE Framework

The Workforce Development Toolkit – a gateway of sorts to many other white papers, best practices, and templates organizations can use for workforce planning and other development activities https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

FedVTE – free cybersecurity training for any HR folks who would want to tell their teams, https://fedvte.usalearning.gov/ and https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

OPM Classification & Qualifications Website, https://www.opm.gov/policy-data-oversight/classification-qualifications/

End of Presentation

Writing Cybersecurity Job Descriptions for the Greatest Impact