NICE Framework v2.2.0

Protection & Defense (PD) Category — Work Role Reference

Complete Task / Knowledge / Skill (TKS) statements for all seven Protection & Defense work roles, with a focused Incident Response vs. Digital Forensics (DFIR) comparison and a cross-role overlap matrix.

Work Role	ID	OPM	TKS
Defensive Cybersecurity	PD-WRL-001	511	205
Digital Forensics	PD-WRL-002	212	181
Incident Response	PD-WRL-003	531	106
Infrastructure Support	PD-WRL-004	521	74
Insider Threat Analysis	PD-WRL-005	TBD	168
Threat Analysis	PD-WRL-006	141	164
Vulnerability Analysis	PD-WRL-007	541	96

Source: NICE Framework Components v2.2.0.xlsx

1. Protection & Defense Category Overview

Protection and Defense (PD): The Protection and Defense (PD) category includes work roles responsible for the identification, assessment, and correction of vulnerabilities and the detection, response to, and remediation of cyber incidents. The seven work roles below span defensive operations, forensics, threat and vulnerability analysis, and infrastructure support.

Defensive Cybersecurity **(PD-WRL-001 · OPM 511)**

Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.

TKS: 205 | Knowledge 124 | Skills 38 | Tasks 43

Digital Forensics **(PD-WRL-002 · OPM 212)**

Responsible for analyzing digital evidence from computer security incidents to derive useful information in support of system and network vulnerability mitigation.

TKS: 181 | Knowledge 93 | Skills 42 | Tasks 46

Incident Response **(PD-WRL-003 · OPM 531)**

Responsible for investigating, analyzing, and responding to network cybersecurity incidents.

TKS: 106 | Knowledge 54 | Skills 23 | Tasks 29

Infrastructure Support **(PD-WRL-004 · OPM 521)**

Responsible for testing, implementing, deploying, maintaining, and administering infrastructure hardware and software for cybersecurity.

TKS: 74 | Knowledge 49 | Skills 11 | Tasks 14

Insider Threat Analysis **(PD-WRL-005 · OPM TBD)**

Responsible for identifying and assessing the capabilities and activities of cybersecurity insider threats; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations.

TKS: 168 | Knowledge 74 | Skills 36 | Tasks 58

Threat Analysis **(PD-WRL-006 · OPM 141)**

Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.

TKS: 164 | Knowledge 75 | Skills 51 | Tasks 38

Vulnerability Analysis **(PD-WRL-007 · OPM 541)**

Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.

TKS: 96 | Knowledge 63 | Skills 18 | Tasks 15

2. Focused Comparison — Incident Response vs. Digital Forensics

Incident Response (PD-WRL-003, OPM 531): 106 TKS • Digital Forensics (PD-WRL-002, OPM 212): 181 TKS

Shared: 48 | **Unique to Incident Response:** 58 | **Unique to Digital Forensics:** 133

2.1 Shared TKS (48)

TKS ID	Type	Description
K0675	Know	Knowledge of risk management processes
K0676	Know	Knowledge of cybersecurity laws and regulations
K0677	Know	Knowledge of cybersecurity policies and procedures
K0678	Know	Knowledge of privacy laws and regulations
K0679	Know	Knowledge of privacy policies and procedures
K0680	Know	Knowledge of cybersecurity principles and practices
K0681	Know	Knowledge of privacy principles and practices
K0682	Know	Knowledge of cybersecurity threats
K0683	Know	Knowledge of cybersecurity vulnerabilities
K0684	Know	Knowledge of cybersecurity threat characteristics
K0701	Know	Knowledge of data backup and recovery policies and procedures
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices
K0724	Know	Knowledge of incident response principles and practices
K0725	Know	Knowledge of incident response tools and techniques
K0726	Know	Knowledge of incident handling tools and techniques
K0751	Know	Knowledge of system threats
K0752	Know	Knowledge of system vulnerabilities
K0770	Know	Knowledge of system administration principles and practices
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices
K0791	Know	Knowledge of defense-in-depth principles and practices
K0837	Know	Knowledge of hardening tools and techniques
K0857	Know	Knowledge of malware analysis tools and techniques
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices
K0915	Know	Knowledge of network architecture principles and practices
K0916	Know	Knowledge of malware analysis principles and practices
K0983	Know	Knowledge of computer networking principles and practices
K1014	Know	Knowledge of network security principles and practices
K1079	Know	Knowledge of web application security risks
S0589	Skil	Skill in preserving digital evidence integrity
S0607	Skil	Skill in collecting digital evidence
S0608	Skil	Skill in processing digital evidence
S0609	Skil	Skill in transporting digital evidence
S0651	Skil	Skill in performing malware analysis
S0821	Skil	Skill in collaborating with internal and external stakeholders
S0854	Skil	Skill in performing data analysis
S0866	Skil	Skill in performing log file analysis
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses
T1084	Task	Identify anomalous network activity
T1118	Task	Identify vulnerabilities
T1119	Task	Recommend vulnerability remediation strategies
T1260	Task	Perform real-time cyber defense incident handling
T1370	Task	Collect intrusion artifacts

TKS ID	Type	Description
T1371	Task	Mitigate potential cyber defense incidents
T1372	Task	Advise law enforcement personnel as technical expert
T1407	Task	Correlate threat assessment data
T1489	Task	Correlate incident data
T1617	Task	Prepare cyber defense reports

2.2 Unique to Incident Response (PD-WRL-003) — 58

TKS ID	Type	Description
K0685	Know	Knowledge of access control principles and practices
K0686	Know	Knowledge of authentication and authorization tools and techniques
K0689	Know	Knowledge of network infrastructure principles and practices
K0709	Know	Knowledge of business continuity and disaster recovery (BCDR) policies and procedures
K0716	Know	Knowledge of host access control (HAC) systems and software
K0717	Know	Knowledge of network access control (NAC) systems and software
K0718	Know	Knowledge of network communications principles and practices
K0732	Know	Knowledge of intrusion detection tools and techniques
K0746	Know	Knowledge of policy-based access controls
K0747	Know	Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)
K0783	Know	Knowledge of network attack characteristics
K0829	Know	Knowledge of account creation policies and procedures
K0830	Know	Knowledge of password policies and procedures
K0832	Know	Knowledge of cyberattack characteristics
K0833	Know	Knowledge of cyberattack actor characteristics
K0844	Know	Knowledge of cyber attack stages
K0845	Know	Knowledge of cyber intrusion activity phases
K0865	Know	Knowledge of data classification standards and best practices
K0866	Know	Knowledge of data classification tools and techniques
K0891	Know	Knowledge of the Open Systems Interconnect (OSI) reference model
K0898	Know	Knowledge of cloud service models and frameworks
K0924	Know	Knowledge of network analysis tools and techniques
K0934	Know	Knowledge of data classification policies and procedures
K0969	Know	Knowledge of cyber-attack tools and techniques
K1049	Know	Knowledge of routing protocols
S0077	Skil	Skill in securing network communications
S0080	Skil	Skill in performing damage assessments
S0483	Skil	Skill in identifying software communications vulnerabilities
S0509	Skil	Skill in evaluating security products
S0544	Skil	Skill in recognizing vulnerabilities
S0547	Skil	Skill in identifying malware
S0548	Skil	Skill in capturing malware
S0549	Skil	Skill in containing malware
S0550	Skil	Skill in reporting malware
S0572	Skil	Skill in detecting host- and network-based intrusions
S0614	Skil	Skill in categorizing types of vulnerabilities
S0615	Skil	Skill in protecting a network against malware
S0688	Skil	Skill in performing network data analysis
S0805	Skil	Skill in designing incident responses
S0806	Skil	Skill in performing incident responses
T0164	Task	Perform cyber defense trend analysis and reporting
T0262	Task	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)
T0510	Task	Coordinate incident response functions
T1085	Task	Identify potential threats to network resources
T1109	Task	Resolve cyber defense incidents
T1110	Task	Coordinate technical support to enterprise-wide cybersecurity defense technicians
T1250	Task	Perform cyber defense incident triage
T1251	Task	Recommend incident remediation strategies

TKS ID	Type	Description
T1252	Task	Determine the scope, urgency, and impact of cyber defense incidents
T1256	Task	Perform forensically sound image collection
T1257	Task	Recommend mitigation and remediation strategies for enterprise systems
T1299	Task	Determine causes of network alerts
T1315	Task	Track cyber defense incidents from initial detection through final resolution
T1316	Task	Document cyber defense incidents from initial detection through final resolution
T1332	Task	Produce incident findings reports
T1333	Task	Communicate incident findings to appropriate constituencies
T1485	Task	Prepare after action reviews (AARs)
T1582	Task	Maintain currency of cyber defense threat conditions

2.3 Unique to Digital Forensics (PD-WRL-002) — 133

TKS ID	Type	Description
K0635	Know	Knowledge of decryption
K0636	Know	Knowledge of decryption tools and techniques
K0637	Know	Knowledge of data repositories
K0674	Know	Knowledge of computer networking protocols
K0696	Know	Knowledge of digital forensic data principles and practices
K0697	Know	Knowledge of encryption algorithm capabilities and applications
K0744	Know	Knowledge of operating system (OS) systems and software
K0759	Know	Knowledge of client and server architecture
K0760	Know	Knowledge of server diagnostic tools and techniques
K0761	Know	Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques
K0786	Know	Knowledge of physical computer components
K0787	Know	Knowledge of computer peripherals
K0793	Know	Knowledge of file extensions
K0794	Know	Knowledge of file system implementation principles and practices
K0795	Know	Knowledge of digital evidence seizure policies and procedures
K0796	Know	Knowledge of digital evidence preservation policies and procedures
K0797	Know	Knowledge of ethical hacking tools and techniques
K0800	Know	Knowledge of evidence admissibility laws and regulations
K0802	Know	Knowledge of chain of custody policies and procedures
K0804	Know	Knowledge of persistent data principles and practices
K0806	Know	Knowledge of machine virtualization tools and techniques
K0807	Know	Knowledge of web mail tools and techniques
K0808	Know	Knowledge of system file characteristics
K0809	Know	Knowledge of digital forensics data characteristics
K0810	Know	Knowledge of deployable forensics principles and practices
K0812	Know	Knowledge of digital communication systems and software
K0817	Know	Knowledge of event correlation tools and techniques
K0840	Know	Knowledge of hardware reverse engineering tools and techniques
K0842	Know	Knowledge of software reverse engineering tools and techniques
K0850	Know	Knowledge of data carving tools and techniques
K0851	Know	Knowledge of reverse engineering principles and practices
K0852	Know	Knowledge of anti-forensics tools and techniques
K0853	Know	Knowledge of forensics lab design principles and practices
K0854	Know	Knowledge of forensics lab design systems and software
K0855	Know	Knowledge of debugging tools and techniques
K0856	Know	Knowledge of filename extension abuse
K0858	Know	Knowledge of virtual machine detection tools and techniques
K0859	Know	Knowledge of encryption tools and techniques
K0892	Know	Knowledge of cyber defense laws and regulations
K0914	Know	Knowledge of binary analysis tools and techniques
K0923	Know	Knowledge of operating system structures and internals
K0939	Know	Knowledge of packet-level analysis tools and techniques
K0959	Know	Knowledge of operational design principles and practices
K0962	Know	Knowledge of targeting laws and regulations
K0963	Know	Knowledge of exploitation laws and regulations
K0977	Know	Knowledge of intelligence collection management tools and techniques
K0979	Know	Knowledge of information searching tools and techniques
K0980	Know	Knowledge of intelligence collection sources
K1004	Know	Knowledge of reporting policies and procedures

TKS ID	Type	Description
K1016	Know	Knowledge of code obfuscation tools and techniques
K1055	Know	Knowledge of digital forensics principles and practices
K1069	Know	Knowledge of virtual machine tools and technologies
K1091	Know	Knowledge of media forensics
K1092	Know	Knowledge of digital forensics tools and techniques
K1115	Know	Knowledge of Chain of Custody (CoC) processes and procedures
K1147	Know	Knowledge of data integrity principles and practices
K1151	Know	Knowledge of digital evidence cataloging tools and techniques
K1152	Know	Knowledge of digital evidence extraction tools and techniques
K1153	Know	Knowledge of digital evidence handling principles and practices
K1154	Know	Knowledge of digital evidence packaging tools and techniques
K1155	Know	Knowledge of digital evidence preservation tools and techniques
K1163	Know	Knowledge of forensic image processing tools and techniques
K1175	Know	Knowledge of network monitoring tools and techniques
K1193	Know	Knowledge of packet analysis tools and techniques
S0156	Skil	Skill in performing packet-level analysis
S0378	Skil	Skill in decrypting information
S0472	Skil	Skill in developing virtual machines
S0473	Skil	Skill in maintaining virtual machines
S0474	Skil	Skill in finding system files
S0475	Skil	Skill in recognizing digital forensics data
S0476	Skil	Skill in identifying filename extension abuse
S0491	Skil	Skill in processing digital forensic data
S0499	Skil	Skill in performing intelligence collection analysis
S0575	Skil	Skill in developing network infrastructure contingency and recovery plans
S0576	Skil	Skill in testing network infrastructure contingency and recovery plans
S0579	Skil	Skill in preparing reports
S0599	Skil	Skill in performing memory dump analysis
S0603	Skil	Skill in identifying forensics data in diverse media
S0604	Skil	Skill in extracting forensics data in diverse media
S0605	Skil	Skill in storing digital evidence
S0606	Skil	Skill in manipulating operating system components
S0611	Skil	Skill in disassembling Personal Computers (PCs)
S0612	Skil	Skill in performing digital forensics analysis
S0621	Skil	Skill in performing binary analysis
S0622	Skil	Skill in implementing one-way hash functions
S0623	Skil	Skill in performing source code analysis
S0624	Skil	Skill in performing volatile data analysis
S0625	Skil	Skill in interpreting debugger results
S0652	Skil	Skill in performing bit-level analysis
S0653	Skil	Skill in creating digital evidence copies
S0671	Skil	Skill in implementing network infrastructure contingency and recovery plans
S0678	Skil	Skill in administering operating systems
S0856	Skil	Skill in performing digital evidence analysis
S0857	Skil	Skill in performing dynamic analysis
S0860	Skil	Skill in performing file system forensic analysis
S0875	Skil	Skill in performing network traffic packet analysis
S0882	Skil	Skill in performing static analysis
S0884	Skil	Skill in performing static malware analysis
T0167	Task	Perform file signature analysis
T0168	Task	Perform data comparison against established database

TKS ID	Type	Description
T0172	Task	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView)
T0173	Task	Perform timeline analysis
T0179	Task	Perform static media analysis
T0182	Task	Perform tier 1, 2, and 3 malware analysis
T0397	Task	Perform Windows registry analysis
T1051	Task	Set up a forensic workstation
T1090	Task	Determine best methods for identifying the perpetrator(s) of a network intrusion
T1102	Task	Identify intrusions
T1103	Task	Analyze intrusions
T1104	Task	Document what is known about intrusions
T1120	Task	Create forensically sound duplicates of evidence
T1121	Task	Decrypt seized data
T1159	Task	Create technical summary of findings reports
T1175	Task	Determine if digital media chain or custody processes meet Federal Rules of Evidence requirements
T1191	Task	Determine relevance of recovered data
T1199	Task	Identify digital evidence for analysis
T1253	Task	Perform dynamic analysis on drives
T1282	Task	Prepare digital media for imaging
T1301	Task	Report forensic artifacts indicative of a particular operating system
T1322	Task	Capture network traffic associated with malicious activities
T1323	Task	Analyze network traffic associated with malicious activities
T1324	Task	Process digital evidence
T1325	Task	Document digital evidence
T1381	Task	Scan digital media for viruses
T1382	Task	Mount a drive image
T1383	Task	Utilize deployable forensics toolkit
T1387	Task	Validate intrusion detection system alerts
T1486	Task	Process forensic images
T1487	Task	Perform file and registry monitoring on running systems
T1488	Task	Enter digital media information into tracking databases
T1490	Task	Prepare cyber defense toolkits
T1510	Task	Preserve digital evidence
T1607	Task	Recover information from forensic data sources

3. Cross-Role TKS Overlap (PD Category)

Each TKS statement can appear in multiple work roles. The table below shows how many TKS are shared between each pair of PD roles (counts only TKS present in BOTH roles).

Role	Defensive	Digital	Incident	Infrastructure	Insider	Threat	Vulnerability
Defensive	205	50	61	44	27	34	59
Digital	50	181	48	27	32	29	34
Incident	61	48	106	39	22	28	48
Infrastructure	44	27	39	74	16	19	33
Insider	27	32	22	16	168	20	19
Threat	34	29	28	19	20	164	23
Vulnerability	59	34	48	33	19	23	96

TKS shared across ≥2 PD roles: **168** of 653 unique PD TKS.

4. Full TKS Appendices — All PD Work Roles

Defensive Cybersecurity (PD-WRL-001) — OPM 511

TKS ID	Type	Description	New
K0068	Know	Knowledge of programming language structures and logic	
K0674	Know	Knowledge of computer networking protocols	
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0685	Know	Knowledge of access control principles and practices	
K0686	Know	Knowledge of authentication and authorization tools and techniques	
K0689	Know	Knowledge of network infrastructure principles and practices	
K0691	Know	Knowledge of cyber defense tools and techniques	
K0692	Know	Knowledge of vulnerability assessment tools and techniques	
K0694	Know	Knowledge of computer algorithm capabilities and applications	
K0698	Know	Knowledge of cryptographic key management principles and practices	
K0707	Know	Knowledge of database systems and software	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0716	Know	Knowledge of host access control (HAC) systems and software	
K0717	Know	Knowledge of network access control (NAC) systems and software	
K0718	Know	Knowledge of network communications principles and practices	
K0723	Know	Knowledge of vulnerability data sources	
K0724	Know	Knowledge of incident response principles and practices	
K0725	Know	Knowledge of incident response tools and techniques	
K0726	Know	Knowledge of incident handling tools and techniques	
K0728	Know	Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices	
K0729	Know	Knowledge of non-repudiation principles and practices	
K0730	Know	Knowledge of cyber safety principles and practices	
K0731	Know	Knowledge of systems security engineering (SSE) principles and practices	
K0732	Know	Knowledge of intrusion detection tools and techniques	
K0736	Know	Knowledge of information technology (IT) security principles and practices	
K0742	Know	Knowledge of identity and access management (IAM) principles and practices	
K0743	Know	Knowledge of new and emerging technologies	
K0744	Know	Knowledge of operating system (OS) systems and software	
K0746	Know	Knowledge of policy-based access controls	
K0747	Know	Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)	
K0749	Know	Knowledge of process engineering principles and practices	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0756	Know	Knowledge of security management principles and practices	
K0757	Know	Knowledge of system design tools and techniques	
K0758	Know	Knowledge of server administration principles and practices	
K0759	Know	Knowledge of client and server architecture	
K0765	Know	Knowledge of software engineering principles and practices	
K0766	Know	Knowledge of data asset management principles and practices	
K0770	Know	Knowledge of system administration principles and practices	
K0772	Know	Knowledge of systems testing and evaluation tools and techniques	
K0773	Know	Knowledge of telecommunications principles and practices	

TKS ID	Type	Description	New
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0779	Know	Knowledge of systems engineering processes	
K0781	Know	Knowledge of virtual private network (VPN) systems and software	
K0783	Know	Knowledge of network attack characteristics	
K0784	Know	Knowledge of insider threat laws and regulations	
K0785	Know	Knowledge of insider threat tools and techniques	
K0788	Know	Knowledge of adversarial tactics principles and practices	
K0789	Know	Knowledge of adversarial tactics tools and techniques	
K0790	Know	Knowledge of adversarial tactics policies and procedures	
K0791	Know	Knowledge of defense-in-depth principles and practices	
K0792	Know	Knowledge of network configurations	
K0793	Know	Knowledge of file extensions	
K0805	Know	Knowledge of command-line tools and techniques	
K0812	Know	Knowledge of digital communication systems and software	
K0813	Know	Knowledge of interpreted and compiled programming language characteristics	
K0815	Know	Knowledge of intelligence collection management processes	
K0816	Know	Knowledge of front-end intelligence collection systems and software	
K0829	Know	Knowledge of account creation policies and procedures	
K0830	Know	Knowledge of password policies and procedures	
K0831	Know	Knowledge of network attack vectors	
K0832	Know	Knowledge of cyberattack characteristics	
K0833	Know	Knowledge of cyberattack actor characteristics	
K0837	Know	Knowledge of hardening tools and techniques	
K0840	Know	Knowledge of hardware reverse engineering tools and techniques	
K0842	Know	Knowledge of software reverse engineering tools and techniques	
K0844	Know	Knowledge of cyber attack stages	
K0845	Know	Knowledge of cyber intrusion activity phases	
K0848	Know	Knowledge of network systems management principles and practices	
K0849	Know	Knowledge of network systems management tools and techniques	
K0851	Know	Knowledge of reverse engineering principles and practices	
K0859	Know	Knowledge of encryption tools and techniques	
K0860	Know	Knowledge of malware signature principles and practices	
K0861	Know	Knowledge of network port capabilities and applications	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0877	Know	Knowledge of application firewall principles and practices	
K0878	Know	Knowledge of network firewall principles and practices	
K0879	Know	Knowledge of industry cybersecurity models and frameworks	
K0880	Know	Knowledge of access control models and frameworks	
K0891	Know	Knowledge of the Open Systems Interconnect (OSI) reference model	
K0892	Know	Knowledge of cyber defense laws and regulations	
K0915	Know	Knowledge of network architecture principles and practices	
K0917	Know	Knowledge of Personally Identifiable Information (PII) data security standards and best practices	
K0918	Know	Knowledge of Payment Card Industry (PCI) data security standards and best practices	
K0919	Know	Knowledge of Personal Health Information (PHI) data security standards and best practices	
K0924	Know	Knowledge of network analysis tools and techniques	
K0928	Know	Knowledge of systems engineering principles and practices	
K0937	Know	Knowledge of countermeasure design principles and practices	
K0938	Know	Knowledge of network mapping principles and practices	
K0939	Know	Knowledge of packet-level analysis tools and techniques	
K0940	Know	Knowledge of subnet tools and techniques	
K0942	Know	Knowledge of cryptology principles and practices	
K0947	Know	Knowledge of computer engineering principles and practices	
K0948	Know	Knowledge of embedded systems and software	
K0950	Know	Knowledge of Intrusion Detection System (IDS) tools and techniques	

TKS ID	Type	Description	New
K0951	Know	Knowledge of Intrusion Prevention System (IPS) tools and techniques	
K0955	Know	Knowledge of penetration testing principles and practices	
K0956	Know	Knowledge of penetration testing tools and techniques	
K0962	Know	Knowledge of targeting laws and regulations	
K0963	Know	Knowledge of exploitation laws and regulations	
K0969	Know	Knowledge of cyber-attack tools and techniques	
K0983	Know	Knowledge of computer networking principles and practices	
K1014	Know	Knowledge of network security principles and practices	
K1079	Know	Knowledge of web application security risks	
K1089	Know	Knowledge of protocol analyzer tools and techniques	
K1108	Know	Knowledge of traceroute tools and techniques	
K1131	Know	Knowledge of cyber defense monitoring tools	
K1132	Know	Knowledge of cyber defense system analysis tools	
K1144	Know	Knowledge of data correlation tools and techniques	
K1168	Know	Knowledge of intrusion set tools and techniques	
K1176	Know	Knowledge of network topologies	
K1181	Know	Knowledge of organizational cybersecurity incident response plans	
K1193	Know	Knowledge of packet analysis tools and techniques	
S0156	Skil	Skill in performing packet-level analysis	
S0483	Skil	Skill in identifying software communications vulnerabilities	
S0490	Skil	Skill in recreating network topologies	
S0509	Skil	Skill in evaluating security products	
S0543	Skil	Skill in scanning for vulnerabilities	
S0544	Skil	Skill in recognizing vulnerabilities	
S0566	Skil	Skill in developing signatures	
S0567	Skil	Skill in deploying signatures	
S0572	Skil	Skill in detecting host- and network-based intrusions	
S0574	Skil	Skill in developing security system controls	
S0578	Skil	Skill in evaluating security designs	
S0593	Skil	Skill in handling incidents	
S0600	Skil	Skill in collecting relevant data from a variety of sources	
S0614	Skil	Skill in categorizing types of vulnerabilities	
S0627	Skil	Skill in reading signatures	
S0651	Skil	Skill in performing malware analysis	
S0667	Skil	Skill in assessing security controls	
S0688	Skil	Skill in performing network data analysis	
S0712	Skil	Skill in evaluating data source quality	
S0722	Skil	Skill in interpreting traceroute results	
S0755	Skil	Skill in reconstructing a network	
S0809	Skil	Skill in utilizing cyber defense service provider information	
S0838	Skil	Skill in identifying anomalous activities	
S0839	Skil	Skill in identifying exploited system weaknesses	
S0840	Skil	Skill in identifying misuse activities	
S0846	Skil	Skill in monitoring system activity	
S0854	Skil	Skill in performing data analysis	
S0857	Skil	Skill in performing dynamic analysis	
S0859	Skil	Skill in performing event correlation	
S0863	Skil	Skill in performing incident analysis	
S0866	Skil	Skill in performing log file analysis	
S0867	Skil	Skill in performing malicious activity analysis	
S0869	Skil	Skill in performing metadata analysis	
S0872	Skil	Skill in performing network data flow analysis	
S0874	Skil	Skill in performing network traffic analysis	
S0875	Skil	Skill in performing network traffic packet analysis	
S0885	Skil	Skill in performing system activity analysis	

TKS ID	Type	Description	New
S0892	Skil	Skill in performing trend analysis	
T0020	Task	Develop content for cyber defense tools	
T0164	Task	Perform cyber defense trend analysis and reporting	
T0292	Task	Recommend computing environment vulnerability corrections	
T0299	Task	Identify network mapping and operating system (OS) fingerprinting activities	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1021	Task	Review cyber defense service provider reporting structure	
T1084	Task	Identify anomalous network activity	
T1085	Task	Identify potential threats to network resources	
T1112	Task	Validate network alerts	
T1119	Task	Recommend vulnerability remediation strategies	
T1176	Task	Determine if cybersecurity-enabled products reduce identified risk to acceptable levels	
T1177	Task	Determine if security control technologies reduce identified risk to acceptable levels	
T1241	Task	Document cybersecurity incidents	
T1242	Task	Escalate incidents that may cause ongoing and immediate impact to the environment	
T1254	Task	Determine the effectiveness of an observed attack	
T1266	Task	Recommend risk mitigation strategies	
T1278	Task	Recommend system modifications	
T1290	Task	Communicate daily network event and activity reports	
T1299	Task	Determine causes of network alerts	
T1347	Task	Detect cybersecurity attacks and intrusions	
T1348	Task	Distinguish between benign and potentially malicious cybersecurity attacks and intrusions	
T1349	Task	Communicate cybersecurity attacks and intrusions alerts	
T1350	Task	Perform continuous monitoring of system activity	
T1351	Task	Determine impact of malicious activity on systems and information	
T1384	Task	Establish intrusion set procedures	
T1386	Task	Analyze network traffic anomalies	
T1387	Task	Validate intrusion detection system alerts	
T1388	Task	Isolate malware	
T1389	Task	Remove malware	
T1390	Task	Identify network device applications and operating systems	
T1391	Task	Reconstruct malicious attacks	
T1406	Task	Construct cyber defense network tool signatures	
T1428	Task	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cybersecurity incidents	
T1539	Task	Analyze organizational cybersecurity posture trends	
T1540	Task	Develop organizational cybersecurity posture trend reports	
T1541	Task	Develop system security posture trend reports	
T1548	Task	Determine adequacy of access controls	
T1582	Task	Maintain currency of cyber defense threat conditions	
T1583	Task	Determine effectiveness of system implementation and testing processes	
T1603	Task	Recommend threat and vulnerability risk mitigation strategies	
T1615	Task	Advise stakeholders on vulnerability compliance	
T1616	Task	Resolve computer security incidents	
T1618	Task	Advise stakeholders on disaster recovery, contingency, and continuity of operations plans	

Digital Forensics (PD-WRL-002) — OPM 212

TKS ID	Type	Description	New
K0635	Know	Knowledge of decryption	
K0636	Know	Knowledge of decryption tools and techniques	
K0637	Know	Knowledge of data repositories	
K0674	Know	Knowledge of computer networking protocols	
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0696	Know	Knowledge of digital forensic data principles and practices	
K0697	Know	Knowledge of encryption algorithm capabilities and applications	
K0701	Know	Knowledge of data backup and recovery policies and procedures	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0724	Know	Knowledge of incident response principles and practices	
K0725	Know	Knowledge of incident response tools and techniques	
K0726	Know	Knowledge of incident handling tools and techniques	
K0744	Know	Knowledge of operating system (OS) systems and software	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0759	Know	Knowledge of client and server architecture	
K0760	Know	Knowledge of server diagnostic tools and techniques	
K0761	Know	Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques	
K0770	Know	Knowledge of system administration principles and practices	
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0786	Know	Knowledge of physical computer components	
K0787	Know	Knowledge of computer peripherals	
K0791	Know	Knowledge of defense-in-depth principles and practices	
K0793	Know	Knowledge of file extensions	
K0794	Know	Knowledge of file system implementation principles and practices	
K0795	Know	Knowledge of digital evidence seizure policies and procedures	
K0796	Know	Knowledge of digital evidence preservation policies and procedures	
K0797	Know	Knowledge of ethical hacking tools and techniques	
K0800	Know	Knowledge of evidence admissibility laws and regulations	
K0802	Know	Knowledge of chain of custody policies and procedures	
K0804	Know	Knowledge of persistent data principles and practices	
K0806	Know	Knowledge of machine virtualization tools and techniques	
K0807	Know	Knowledge of web mail tools and techniques	
K0808	Know	Knowledge of system file characteristics	
K0809	Know	Knowledge of digital forensics data characteristics	
K0810	Know	Knowledge of deployable forensics principles and practices	
K0812	Know	Knowledge of digital communication systems and software	
K0817	Know	Knowledge of event correlation tools and techniques	
K0837	Know	Knowledge of hardening tools and techniques	
K0840	Know	Knowledge of hardware reverse engineering tools and techniques	
K0842	Know	Knowledge of software reverse engineering tools and techniques	
K0850	Know	Knowledge of data carving tools and techniques	
K0851	Know	Knowledge of reverse engineering principles and practices	
K0852	Know	Knowledge of anti-forensics tools and techniques	

TKS ID	Type	Description	New
K0853	Know	Knowledge of forensics lab design principles and practices	
K0854	Know	Knowledge of forensics lab design systems and software	
K0855	Know	Knowledge of debugging tools and techniques	
K0856	Know	Knowledge of filename extension abuse	
K0857	Know	Knowledge of malware analysis tools and techniques	
K0858	Know	Knowledge of virtual machine detection tools and techniques	
K0859	Know	Knowledge of encryption tools and techniques	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0892	Know	Knowledge of cyber defense laws and regulations	
K0914	Know	Knowledge of binary analysis tools and techniques	
K0915	Know	Knowledge of network architecture principles and practices	
K0916	Know	Knowledge of malware analysis principles and practices	
K0923	Know	Knowledge of operating system structures and internals	
K0939	Know	Knowledge of packet-level analysis tools and techniques	
K0959	Know	Knowledge of operational design principles and practices	
K0962	Know	Knowledge of targeting laws and regulations	
K0963	Know	Knowledge of exploitation laws and regulations	
K0977	Know	Knowledge of intelligence collection management tools and techniques	
K0979	Know	Knowledge of information searching tools and techniques	
K0980	Know	Knowledge of intelligence collection sources	
K0983	Know	Knowledge of computer networking principles and practices	
K1004	Know	Knowledge of reporting policies and procedures	
K1014	Know	Knowledge of network security principles and practices	
K1016	Know	Knowledge of code obfuscation tools and techniques	
K1055	Know	Knowledge of digital forensics principles and practices	
K1069	Know	Knowledge of virtual machine tools and technologies	
K1079	Know	Knowledge of web application security risks	
K1091	Know	Knowledge of media forensics	
K1092	Know	Knowledge of digital forensics tools and techniques	
K1115	Know	Knowledge of Chain of Custody (CoC) processes and procedures	
K1147	Know	Knowledge of data integrity principles and practices	
K1151	Know	Knowledge of digital evidence cataloging tools and techniques	
K1152	Know	Knowledge of digital evidence extraction tools and techniques	
K1153	Know	Knowledge of digital evidence handling principles and practices	
K1154	Know	Knowledge of digital evidence packaging tools and techniques	
K1155	Know	Knowledge of digital evidence preservation tools and techniques	
K1163	Know	Knowledge of forensic image processing tools and techniques	
K1175	Know	Knowledge of network monitoring tools and techniques	
K1193	Know	Knowledge of packet analysis tools and techniques	
S0156	Skil	Skill in performing packet-level analysis	
S0378	Skil	Skill in decrypting information	
S0472	Skil	Skill in developing virtual machines	
S0473	Skil	Skill in maintaining virtual machines	
S0474	Skil	Skill in finding system files	
S0475	Skil	Skill in recognizing digital forensics data	
S0476	Skil	Skill in identifying filename extension abuse	
S0491	Skil	Skill in processing digital forensic data	
S0499	Skil	Skill in performing intelligence collection analysis	
S0575	Skil	Skill in developing network infrastructure contingency and recovery plans	
S0576	Skil	Skill in testing network infrastructure contingency and recovery plans	
S0579	Skil	Skill in preparing reports	
S0589	Skil	Skill in preserving digital evidence integrity	
S0599	Skil	Skill in performing memory dump analysis	
S0603	Skil	Skill in identifying forensics data in diverse media	

TKS ID	Type	Description	New
S0604	Skil	Skill in extracting forensics data in diverse media	
S0605	Skil	Skill in storing digital evidence	
S0606	Skil	Skill in manipulating operating system components	
S0607	Skil	Skill in collecting digital evidence	
S0608	Skil	Skill in processing digital evidence	
S0609	Skil	Skill in transporting digital evidence	
S0611	Skil	Skill in disassembling Personal Computers (PCs)	
S0612	Skil	Skill in performing digital forensics analysis	
S0621	Skil	Skill in performing binary analysis	
S0622	Skil	Skill in implementing one-way hash functions	
S0623	Skil	Skill in performing source code analysis	
S0624	Skil	Skill in performing volatile data analysis	
S0625	Skil	Skill in interpreting debugger results	
S0651	Skil	Skill in performing malware analysis	
S0652	Skil	Skill in performing bit-level analysis	
S0653	Skil	Skill in creating digital evidence copies	
S0671	Skil	Skill in implementing network infrastructure contingency and recovery plans	
S0678	Skil	Skill in administering operating systems	
S0821	Skil	Skill in collaborating with internal and external stakeholders	
S0854	Skil	Skill in performing data analysis	
S0856	Skil	Skill in performing digital evidence analysis	
S0857	Skil	Skill in performing dynamic analysis	
S0860	Skil	Skill in performing file system forensic analysis	
S0866	Skil	Skill in performing log file analysis	
S0875	Skil	Skill in performing network traffic packet analysis	
S0882	Skil	Skill in performing static analysis	
S0884	Skil	Skill in performing static malware analysis	
T0167	Task	Perform file signature analysis	
T0168	Task	Perform data comparison against established database	
T0172	Task	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView)	
T0173	Task	Perform timeline analysis	
T0179	Task	Perform static media analysis	
T0182	Task	Perform tier 1, 2, and 3 malware analysis	
T0397	Task	Perform Windows registry analysis	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1051	Task	Set up a forensic workstation	
T1084	Task	Identify anomalous network activity	
T1090	Task	Determine best methods for identifying the perpetrator(s) of a network intrusion	
T1102	Task	Identify intrusions	
T1103	Task	Analyze intrusions	
T1104	Task	Document what is known about intrusions	
T1118	Task	Identify vulnerabilities	
T1119	Task	Recommend vulnerability remediation strategies	
T1120	Task	Create forensically sound duplicates of evidence	
T1121	Task	Decrypt seized data	
T1159	Task	Create technical summary of findings reports	
T1175	Task	Determine if digital media chain or custody processes meet Federal Rules of Evidence requirements	
T1191	Task	Determine relevance of recovered data	
T1199	Task	Identify digital evidence for analysis	
T1253	Task	Perform dynamic analysis on drives	
T1260	Task	Perform real-time cyber defense incident handling	
T1282	Task	Prepare digital media for imaging	
T1301	Task	Report forensic artifacts indicative of a particular operating system	
T1322	Task	Capture network traffic associated with malicious activities	
T1323	Task	Analyze network traffic associated with malicious activities	

TKS ID	Type	Description	New
T1324	Task	Process digital evidence	
T1325	Task	Document digital evidence	
T1370	Task	Collect intrusion artifacts	
T1371	Task	Mitigate potential cyber defense incidents	
T1372	Task	Advise law enforcement personnel as technical expert	
T1381	Task	Scan digital media for viruses	
T1382	Task	Mount a drive image	
T1383	Task	Utilize deployable forensics toolkit	
T1387	Task	Validate intrusion detection system alerts	
T1407	Task	Correlate threat assessment data	
T1486	Task	Process forensic images	
T1487	Task	Perform file and registry monitoring on running systems	
T1488	Task	Enter digital media information into tracking databases	
T1489	Task	Correlate incident data	
T1490	Task	Prepare cyber defense toolkits	
T1510	Task	Preserve digital evidence	
T1607	Task	Recover information from forensic data sources	
T1617	Task	Prepare cyber defense reports	

Incident Response (PD-WRL-003) — OPM 531

TKS ID	Type	Description	New
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0685	Know	Knowledge of access control principles and practices	
K0686	Know	Knowledge of authentication and authorization tools and techniques	
K0689	Know	Knowledge of network infrastructure principles and practices	
K0701	Know	Knowledge of data backup and recovery policies and procedures	
K0709	Know	Knowledge of business continuity and disaster recovery (BCDR) policies and procedures	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0716	Know	Knowledge of host access control (HAC) systems and software	
K0717	Know	Knowledge of network access control (NAC) systems and software	
K0718	Know	Knowledge of network communications principles and practices	
K0724	Know	Knowledge of incident response principles and practices	
K0725	Know	Knowledge of incident response tools and techniques	
K0726	Know	Knowledge of incident handling tools and techniques	
K0732	Know	Knowledge of intrusion detection tools and techniques	
K0746	Know	Knowledge of policy-based access controls	
K0747	Know	Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0770	Know	Knowledge of system administration principles and practices	
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0783	Know	Knowledge of network attack characteristics	
K0791	Know	Knowledge of defense-in-depth principles and practices	
K0829	Know	Knowledge of account creation policies and procedures	
K0830	Know	Knowledge of password policies and procedures	
K0832	Know	Knowledge of cyberattack characteristics	
K0833	Know	Knowledge of cyberattack actor characteristics	
K0837	Know	Knowledge of hardening tools and techniques	
K0844	Know	Knowledge of cyber attack stages	
K0845	Know	Knowledge of cyber intrusion activity phases	
K0857	Know	Knowledge of malware analysis tools and techniques	
K0865	Know	Knowledge of data classification standards and best practices	
K0866	Know	Knowledge of data classification tools and techniques	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0891	Know	Knowledge of the Open Systems Interconnect (OSI) reference model	
K0898	Know	Knowledge of cloud service models and frameworks	
K0915	Know	Knowledge of network architecture principles and practices	
K0916	Know	Knowledge of malware analysis principles and practices	
K0924	Know	Knowledge of network analysis tools and techniques	
K0934	Know	Knowledge of data classification policies and procedures	
K0969	Know	Knowledge of cyber-attack tools and techniques	
K0983	Know	Knowledge of computer networking principles and practices	
K1014	Know	Knowledge of network security principles and practices	
K1049	Know	Knowledge of routing protocols	

TKS ID	Type	Description	New
K1079	Know	Knowledge of web application security risks	
S0077	Skil	Skill in securing network communications	
S0080	Skil	Skill in performing damage assessments	
S0483	Skil	Skill in identifying software communications vulnerabilities	
S0509	Skil	Skill in evaluating security products	
S0544	Skil	Skill in recognizing vulnerabilities	
S0547	Skil	Skill in identifying malware	
S0548	Skil	Skill in capturing malware	
S0549	Skil	Skill in containing malware	
S0550	Skil	Skill in reporting malware	
S0572	Skil	Skill in detecting host- and network-based intrusions	
S0589	Skil	Skill in preserving digital evidence integrity	
S0607	Skil	Skill in collecting digital evidence	
S0608	Skil	Skill in processing digital evidence	
S0609	Skil	Skill in transporting digital evidence	
S0614	Skil	Skill in categorizing types of vulnerabilities	
S0615	Skil	Skill in protecting a network against malware	
S0651	Skil	Skill in performing malware analysis	
S0688	Skil	Skill in performing network data analysis	
S0805	Skil	Skill in designing incident responses	
S0806	Skil	Skill in performing incident responses	
S0821	Skil	Skill in collaborating with internal and external stakeholders	
S0854	Skil	Skill in performing data analysis	
S0866	Skil	Skill in performing log file analysis	
T0164	Task	Perform cyber defense trend analysis and reporting	
T0262	Task	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)	
T0510	Task	Coordinate incident response functions	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1084	Task	Identify anomalous network activity	
T1085	Task	Identify potential threats to network resources	
T1109	Task	Resolve cyber defense incidents	
T1110	Task	Coordinate technical support to enterprise-wide cybersecurity defense technicians	
T1118	Task	Identify vulnerabilities	
T1119	Task	Recommend vulnerability remediation strategies	
T1250	Task	Perform cyber defense incident triage	
T1251	Task	Recommend incident remediation strategies	
T1252	Task	Determine the scope, urgency, and impact of cyber defense incidents	
T1256	Task	Perform forensically sound image collection	
T1257	Task	Recommend mitigation and remediation strategies for enterprise systems	
T1260	Task	Perform real-time cyber defense incident handling	
T1299	Task	Determine causes of network alerts	
T1315	Task	Track cyber defense incidents from initial detection through final resolution	
T1316	Task	Document cyber defense incidents from initial detection through final resolution	
T1332	Task	Produce incident findings reports	
T1333	Task	Communicate incident findings to appropriate constituencies	
T1370	Task	Collect intrusion artifacts	
T1371	Task	Mitigate potential cyber defense incidents	
T1372	Task	Advise law enforcement personnel as technical expert	
T1407	Task	Correlate threat assessment data	
T1485	Task	Prepare after action reviews (AARs)	
T1489	Task	Correlate incident data	
T1582	Task	Maintain currency of cyber defense threat conditions	
T1617	Task	Prepare cyber defense reports	

Infrastructure Support (PD-WRL-004) — OPM 521

TKS ID	Type	Description	New
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0685	Know	Knowledge of access control principles and practices	
K0686	Know	Knowledge of authentication and authorization tools and techniques	
K0701	Know	Knowledge of data backup and recovery policies and procedures	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0716	Know	Knowledge of host access control (HAC) systems and software	
K0717	Know	Knowledge of network access control (NAC) systems and software	
K0724	Know	Knowledge of incident response principles and practices	
K0725	Know	Knowledge of incident response tools and techniques	
K0726	Know	Knowledge of incident handling tools and techniques	
K0728	Know	Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices	
K0729	Know	Knowledge of non-repudiation principles and practices	
K0730	Know	Knowledge of cyber safety principles and practices	
K0734	Know	Knowledge of Risk Management Framework (RMF) requirements	
K0746	Know	Knowledge of policy-based access controls	
K0747	Know	Knowledge of Risk Adaptive (Adaptable) Access Controls (RAdAC)	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0770	Know	Knowledge of system administration principles and practices	
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0781	Know	Knowledge of virtual private network (VPN) systems and software	
K0783	Know	Knowledge of network attack characteristics	
K0791	Know	Knowledge of defense-in-depth principles and practices	
K0792	Know	Knowledge of network configurations	
K0811	Know	Knowledge of web filtering systems and software	
K0829	Know	Knowledge of account creation policies and procedures	
K0830	Know	Knowledge of password policies and procedures	
K0837	Know	Knowledge of hardening tools and techniques	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0881	Know	Knowledge of learning assessment tools and techniques	
K0891	Know	Knowledge of the Open Systems Interconnect (OSI) reference model	
K0915	Know	Knowledge of network architecture principles and practices	
K0925	Know	Knowledge of wireless communication tools and techniques	
K0926	Know	Knowledge of signal jamming tools and techniques	
K0950	Know	Knowledge of Intrusion Detection System (IDS) tools and techniques	
K0951	Know	Knowledge of Intrusion Prevention System (IPS) tools and techniques	
K0983	Know	Knowledge of computer networking principles and practices	
K1014	Know	Knowledge of network security principles and practices	
K1211	Know	Knowledge of security assessment authorization requirements	
S0077	Skil	Skill in securing network communications	
S0552	Skil	Skill in applying host access controls	
S0553	Skil	Skill in applying network access controls	
S0592	Skil	Skill in tuning network sensors	

TKS ID	Type	Description	New
S0593	Skil	Skill in handling incidents	
S0596	Skil	Skill in encrypting network communications	
S0615	Skil	Skill in protecting a network against malware	
S0643	Skil	Skill in applying hardening techniques	
S0645	Skil	Skill in troubleshooting cyber defense infrastructure anomalies	
S0831	Skil	Skill in configuring hardware	
S0898	Skil	Skill in testing hardware	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1111	Task	Administer rule and signature updates for specialized cyber defense applications	
T1267	Task	Perform system administration on specialized cyber defense applications and systems	
T1268	Task	Administer Virtual Private Network (VPN) devices	
T1352	Task	Coordinate critical cyber defense infrastructure protection measures	
T1353	Task	Prioritize critical cyber defense infrastructure resources	
T1432	Task	Build dedicated cyber defense hardware	
T1433	Task	Install dedicated cyber defense hardware	
T1442	Task	Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure	
T1503	Task	Evaluate platforms managed by service providers	
T1515	Task	Manage network access control lists on specialized cyber defense systems	
T1555	Task	Implement cyber defense tools	
T1561	Task	Implement dedicated cyber defense systems	
T1562	Task	Document system requirements	

Insider Threat Analysis (PD-WRL-005) — OPM TBD

TKS ID	Type	Description	New
K0636	Know	Knowledge of decryption tools and techniques	
K0637	Know	Knowledge of data repositories	
K0656	Know	Knowledge of network collection tools and techniques	
K0657	Know	Knowledge of network collection policies and procedures	
K0674	Know	Knowledge of computer networking protocols	
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0689	Know	Knowledge of network infrastructure principles and practices	
K0707	Know	Knowledge of database systems and software	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0721	Know	Knowledge of risk management principles and practices	
K0734	Know	Knowledge of Risk Management Framework (RMF) requirements	
K0735	Know	Knowledge of risk management models and frameworks	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0784	Know	Knowledge of insider threat laws and regulations	
K0785	Know	Knowledge of insider threat tools and techniques	
K0802	Know	Knowledge of chain of custody policies and procedures	
K0862	Know	Knowledge of data remediation tools and techniques	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0909	Know	Knowledge of abnormal physical and physiological behaviors	
K1014	Know	Knowledge of network security principles and practices	
K1023	Know	Knowledge of network exploitation tools and techniques	
K1031	Know	Knowledge of risk mitigation tools and techniques	
K1085	Know	Knowledge of exploitation tools and techniques	
K1096	Know	Knowledge of data analysis tools and techniques	
K1151	Know	Knowledge of digital evidence cataloging tools and techniques	
K1152	Know	Knowledge of digital evidence extraction tools and techniques	
K1154	Know	Knowledge of digital evidence packaging tools and techniques	
K1155	Know	Knowledge of digital evidence preservation tools and techniques	
K1180	Know	Knowledge of organizational cybersecurity goals and objectives	
K1188	Know	Knowledge of organizational policies and procedures	
K1197	Know	Knowledge of priority intelligence requirements	
K1209	Know	Knowledge of risk mitigation principles and practices	
K1241	Know	Knowledge of cultural, political, and organizational assets	
K1242	Know	Knowledge of cybersecurity review processes and procedures	
K1243	Know	Knowledge of cybersecurity threat remediation principles and practices	
K1244	Know	Knowledge of cybersecurity tools and techniques	
K1245	Know	Knowledge of data exfiltration tools and techniques	
K1246	Know	Knowledge of data handling tools and techniques	
K1247	Know	Knowledge of data monitoring tools and techniques	
K1248	Know	Knowledge of digital and physical security vulnerabilities	
K1249	Know	Knowledge of digital and physical security vulnerability remediation principles and practices	
K1250	Know	Knowledge of external organization roles and responsibilities	
K1251	Know	Knowledge of external referrals policies and procedures	

TKS ID	Type	Description	New
K1252	Know	Knowledge of high value asset characteristics	
K1254	Know	Knowledge of insider threat hub policies and procedures	
K1255	Know	Knowledge of insider threat hub operations	
K1256	Know	Knowledge of insider threat operational indicators	
K1257	Know	Knowledge of insider threat policies and procedures	
K1258	Know	Knowledge of insider threat tactics	
K1259	Know	Knowledge of insider threat targets	
K1260	Know	Knowledge of intelligence laws and regulations	
K1261	Know	Knowledge of known insider attacks	
K1262	Know	Knowledge of network endpoints	
K1263	Know	Knowledge of notification policies and procedures	
K1265	Know	Knowledge of organizational objectives, resources, and capabilities	
K1267	Know	Knowledge of previously referred potential insider threats	
K1268	Know	Knowledge of risk reduction metrics	
K1269	Know	Knowledge of security information and event management (SIEM) tools and techniques	
K1270	Know	Knowledge of suspicious activity response processes	
K1271	Know	Knowledge of system alert policies and procedures	
K1272	Know	Knowledge of system components	
K1273	Know	Knowledge of threat investigation policies and procedures	
K1274	Know	Knowledge of threat modeling tools and techniques	
K1275	Know	Knowledge of User Activity Monitoring (UAM) tools and techniques	
S0378	Skil	Skill in decrypting information	
S0391	Skil	Skill in creating technical documentation	
S0442	Skil	Skill in collecting network data	
S0477	Skil	Skill in identifying anomalous activity	
S0540	Skil	Skill in identifying network threats	
S0558	Skil	Skill in developing algorithms	
S0559	Skil	Skill in performing data structure analysis	
S0579	Skil	Skill in preparing reports	
S0588	Skil	Skill in performing threat modeling	
S0610	Skil	Skill in communicating effectively	
S0688	Skil	Skill in performing network data analysis	
S0690	Skil	Skill in performing midpoint collection data analysis	
S0728	Skil	Skill in preparing briefings	
S0748	Skil	Skill in querying data	
S0791	Skil	Skill in presenting to an audience	
S0817	Skil	Skill in building internal and external relationships	
S0821	Skil	Skill in collaborating with internal and external stakeholders	
S0848	Skil	Skill in performing behavioral analysis	
S0854	Skil	Skill in performing data analysis	
S0866	Skil	Skill in performing log file analysis	
S0874	Skil	Skill in performing network traffic analysis	
S0890	Skil	Skill in performing threat analysis	
S0896	Skil	Skill in recognizing behavioral patterns	
S0900	Skil	Skill in analyzing information from multiple sources	
S0902	Skil	Skill in building relationships remotely and in person	
S0904	Skil	Skill in correlating data from multiple tools	
S0905	Skil	Skill in determining what information may helpful to a specific audience	
S0906	Skil	Skill in identifying insider risk security gaps	
S0907	Skil	Skill in identifying insider threats	
S0908	Skil	Skill in determining the importance of assets	
S0909	Skil	Skill in integrating information from multiple sources	
S0910	Skil	Skill in performing cyberintelligence data analysis	
S0911	Skil	Skill in performing data queries	
S0912	Skil	Skill in performing human behavioral analysis	

TKS ID	Type	Description	New
S0913	Skil	Skill in performing link analysis	
S0916	Skil	Skill in recognizing recurring threat incidents	
T1056	Task	Acquire resources to support cybersecurity program goals and objectives	
T1057	Task	Conduct an effective enterprise continuity of operations program	
T1062	Task	Contribute insider threat expertise to organizational cybersecurity awareness program	
T1084	Task	Identify anomalous network activity	
T1085	Task	Identify potential threats to network resources	
T1160	Task	Develop risk mitigation strategies	
T1162	Task	Recommend security changes to systems and system components	
T1227	Task	Manage cybersecurity budget, staffing, and contracting	
T1266	Task	Recommend risk mitigation strategies	
T1324	Task	Process digital evidence	
T1325	Task	Document digital evidence	
T1439	Task	Assess the behavior of individual victims, witnesses, or suspects during cybersecurity investigations	
T1510	Task	Preserve digital evidence	
T1592	Task	Conduct cybersecurity reviews	
T1690	Task	Identify exploitable technical or operational vulnerabilities	
T1712	Task	Recommend potential courses of action	
T1737	Task	Develop intelligence collection strategies	
T1743	Task	Identify information collection gaps	
T1799	Task	Notify appropriate personnel of imminent hostile intentions or activities	
T1801	Task	Determine validity and relevance of information	
T1969	Task	Document system alerts	
T1970	Task	Escalate system alerts that may indicate risks	
T1971	Task	Disseminate anomalous activity reports to the insider threat hub	
T1973	Task	Conduct independent comprehensive assessments of target-specific information	
T1974	Task	Conduct insider threat risk assessments	
T1975	Task	Prepare insider threat briefings	
T1976	Task	Recommend risk mitigation courses of action (CoA)	
T1977	Task	Coordinate with internal and external incident management partners across jurisdictions	
T1978	Task	Recommend improvements to insider threat detection processes	
T1979	Task	Collect digital evidence that meets priority intelligence requirements	
T1980	Task	Develop digital evidence reports for internal and external partners	
T1981	Task	Develop elicitation indicators	
T1982	Task	Identify high value assets	
T1983	Task	Identify potential insider threats	
T1985	Task	Identify imminent or hostile intentions or activities	
T1986	Task	Develop a continuously updated overview of an incident throughout the incident's life cycle	
T1987	Task	Develop insider threat cyber operations indicators	
T1988	Task	Integrate information from cyber resources, internal partners, and external partners	
T1989	Task	Advise insider threat hub inquiries	
T1990	Task	Conduct cybersecurity insider threat inquiries	
T1991	Task	Deliver all-source cyber operations and intelligence indications and warnings	
T1992	Task	Interpret network activity for intelligence value	
T1993	Task	Monitor network activity for vulnerabilities	
T1994	Task	Identify potential insider risks to networks	
T1995	Task	Document potential insider risks to networks	
T1996	Task	Report network vulnerabilities	
T1997	Task	Develop insider threat investigation plans	
T1998	Task	Investigate alleged insider threat cybersecurity policy violations	
T1999	Task	Refer cases on active insider threat activities to law enforcement investigators	
T2001	Task	Establish an insider threat risk management assessment program	
T2003	Task	Evaluate organizational insider risk response capabilities	
T2004	Task	Document insider threat information sources	
T2005	Task	Conduct insider threat studies	

TKS ID	Type	Description	New
T2006	Task	Identify potential targets for exploitation	
T2007	Task	Analyze potential targets for exploitation	
T2009	Task	Develop insider threat targets	
T2010	Task	Maintain User Activity Monitoring (UAM) tools	
T2011	Task	Monitor the output from User Activity Monitoring (UAM) tools	

Threat Analysis (PD-WRL-006) — OPM 141

TKS ID	Type	Description	New
K0480	Know	Knowledge of malware	
K0655	Know	Knowledge of intelligence fusion	
K0658	Know	Knowledge of cognitive biases	
K0674	Know	Knowledge of computer networking protocols	
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0689	Know	Knowledge of network infrastructure principles and practices	
K0690	Know	Knowledge of requirements analysis principles and practices	
K0697	Know	Knowledge of encryption algorithm capabilities and applications	
K0718	Know	Knowledge of network communications principles and practices	
K0719	Know	Knowledge of human-computer interaction (HCI) principles and practices	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0766	Know	Knowledge of data asset management principles and practices	
K0773	Know	Knowledge of telecommunications principles and practices	
K0786	Know	Knowledge of physical computer components	
K0787	Know	Knowledge of computer peripherals	
K0788	Know	Knowledge of adversarial tactics principles and practices	
K0789	Know	Knowledge of adversarial tactics tools and techniques	
K0790	Know	Knowledge of adversarial tactics policies and procedures	
K0792	Know	Knowledge of network configurations	
K0806	Know	Knowledge of machine virtualization tools and techniques	
K0812	Know	Knowledge of digital communication systems and software	
K0818	Know	Knowledge of new and emerging cybersecurity risks	
K0825	Know	Knowledge of threat vector characteristics	
K0831	Know	Knowledge of network attack vectors	
K0844	Know	Knowledge of cyber attack stages	
K0845	Know	Knowledge of cyber intrusion activity phases	
K0857	Know	Knowledge of malware analysis tools and techniques	
K0858	Know	Knowledge of virtual machine detection tools and techniques	
K0865	Know	Knowledge of data classification standards and best practices	
K0866	Know	Knowledge of data classification tools and techniques	
K0915	Know	Knowledge of network architecture principles and practices	
K0916	Know	Knowledge of malware analysis principles and practices	
K0925	Know	Knowledge of wireless communication tools and techniques	
K0926	Know	Knowledge of signal jamming tools and techniques	
K0934	Know	Knowledge of data classification policies and procedures	
K0960	Know	Knowledge of content management system (CMS) capabilities and applications	
K0969	Know	Knowledge of cyber-attack tools and techniques	
K0983	Know	Knowledge of computer networking principles and practices	
K0984	Know	Knowledge of web security principles and practices	
K0989	Know	Knowledge of intelligence information repositories	
K0990	Know	Knowledge of cyber operations principles and practices	
K0994	Know	Knowledge of denial and deception tools and techniques	
K1002	Know	Knowledge of supervisory control and data acquisition (SCADA) systems and software	

TKS ID	Type	Description	New
K1005	Know	Knowledge of intelligence collection capabilities and applications	
K1007	Know	Knowledge of intelligence requirements tasking systems and software	
K1008	Know	Knowledge of intelligence support activities	
K1009	Know	Knowledge of threat intelligence principles and practices	
K1010	Know	Knowledge of intelligence policies and procedures	
K1011	Know	Knowledge of network addressing principles and practices	
K1014	Know	Knowledge of network security principles and practices	
K1019	Know	Knowledge of operations security (OPSEC) principles and practices	
K1025	Know	Knowledge of decision-making policies and procedures	
K1028	Know	Knowledge of target development principles and practices	
K1035	Know	Knowledge of target research tools and techniques	
K1049	Know	Knowledge of routing protocols	
K1059	Know	Knowledge of request for information processes	
K1066	Know	Knowledge of threat behaviors	
K1067	Know	Knowledge of target behaviors	
K1068	Know	Knowledge of threat systems and software	
K1069	Know	Knowledge of virtual machine tools and technologies	
K1100	Know	Knowledge of analytical tools and techniques	
K1101	Know	Knowledge of analytics	
K1109	Know	Knowledge of virtual collaborative workspace tools and techniques	
K1113	Know	Knowledge of blue force tracking	
K1197	Know	Knowledge of priority intelligence requirements	
S0111	Skil	Skill in interfacing with customers	
S0194	Skil	Skill in conducting non-attributable research	
S0385	Skil	Skill in communicating complex concepts	
S0430	Skil	Skill in collaborating with others	
S0433	Skil	Skill in creating analytics	
S0434	Skil	Skill in extrapolating from incomplete data sets	
S0435	Skil	Skill in analyzing large data sets	
S0436	Skil	Skill in creating target intelligence products	
S0438	Skil	Skill in functioning effectively in a dynamic, fast-paced environment	
S0443	Skil	Skill in mitigating cognitive biases	
S0444	Skil	Skill in mitigating deception in reporting and analysis	
S0446	Skil	Skill in mimicking threat actors	
S0472	Skil	Skill in developing virtual machines	
S0473	Skil	Skill in maintaining virtual machines	
S0494	Skil	Skill in performing operational environment analysis	
S0505	Skil	Skill in performing intrusion data analysis	
S0506	Skil	Skill in identifying customer information needs	
S0509	Skil	Skill in evaluating security products	
S0511	Skil	Skill in establishing priorities	
S0512	Skil	Skill in extracting metadata	
S0514	Skil	Skill in preparing operational environments	
S0516	Skil	Skill in performing threat emulation tactics	
S0517	Skil	Skill in anticipating threats	
S0535	Skil	Skill in performing threat factor analysis	
S0537	Skil	Skill in designing wireless communications systems	
S0540	Skil	Skill in identifying network threats	
S0555	Skil	Skill in performing capabilities analysis	
S0556	Skil	Skill in performing requirements analysis	
S0579	Skil	Skill in preparing reports	
S0600	Skil	Skill in collecting relevant data from a variety of sources	
S0633	Skil	Skill in developing position qualification requirements	
S0673	Skil	Skill in translating operational requirements into security controls	
S0696	Skil	Skill in conducting deep web research	

TKS ID	Type	Description	New
S0702	Skil	Skill in defining an operational environment	
S0704	Skil	Skill in performing target analysis	
S0709	Skil	Skill in developing analytics	
S0712	Skil	Skill in evaluating data source quality	
S0713	Skil	Skill in evaluating information quality	
S0718	Skil	Skill in identifying cybersecurity threats	
S0719	Skil	Skill in identifying intelligence gaps	
S0724	Skil	Skill in managing client relationships	
S0728	Skil	Skill in preparing briefings	
S0748	Skil	Skill in querying data	
S0751	Skil	Skill in conducting open-source searches	
S0756	Skil	Skill in incorporating feedback	
S0765	Skil	Skill in converting intelligence requirements into intelligence production tasks	
S0777	Skil	Skill in developing collection strategies	
S0779	Skil	Skill in determining information requirements	
S0791	Skil	Skill in presenting to an audience	
S0869	Skil	Skill in performing metadata analysis	
S0876	Skil	Skill in performing nodal analysis	
T0569	Task	Answer requests for information	
T0685	Task	Evaluate threat decision-making processes	
T0698	Task	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers	
T0707	Task	Generate requests for information	
T0718	Task	Identify intelligence gaps and shortfalls	
T0751	Task	Monitor open source websites for hostile content directed towards organizational or partner interests	
T0845	Task	Identify cyber threat tactics and methodologies	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1035	Task	Determine how threat activity groups employ encryption to support their operations	
T1053	Task	Identify and characterize intrusion activities against a victim or target	
T1054	Task	Scope analysis reports to various audiences that accounts for data sharing classification restrictions	
T1055	Task	Determine if priority information requirements are satisfied	
T1640	Task	Determine effectiveness of intelligence collection operations	
T1641	Task	Recommend adjustments to intelligence collection strategies	
T1643	Task	Develop common operational pictures	
T1644	Task	Develop cyber operations indicators	
T1645	Task	Coordinate all-source collection activities	
T1646	Task	Validate all-source collection requirements and plans	
T1647	Task	Develop priority information requirements	
T1651	Task	Prepare threat and target briefings	
T1652	Task	Prepare threat and target situational updates	
T1686	Task	Identify intelligence requirements	
T1762	Task	Modify collection requirements	
T1763	Task	Determine effectiveness of collection requirements	
T1765	Task	Monitor changes to designated cyber operations warning problem sets	
T1766	Task	Prepare change reports for designated cyber operations warning problem sets	
T1767	Task	Monitor threat activities	
T1768	Task	Prepare threat activity reports	
T1770	Task	Report on adversarial activities that fulfill priority information requirements	
T1772	Task	Identify indications and warnings of target communication changes or processing failures	
T1775	Task	Prepare cyber operations intelligence reports	
T1776	Task	Prepare indications and warnings intelligence reports	
T1792	Task	Assess effectiveness of intelligence production	
T1793	Task	Assess effectiveness of intelligence reporting	
T1798	Task	Provide intelligence analysis and support	
T1799	Task	Notify appropriate personnel of imminent hostile intentions or activities	

TKS ID	Type	Description	New
T1804	Task	Prepare network intrusion reports	
T1835	Task	Determine if intelligence requirements and collection plans are accurate and up-to-date	

Vulnerability Analysis (PD-WRL-007) — OPM 541

TKS ID	Type	Description	New
K0674	Know	Knowledge of computer networking protocols	
K0675	Know	Knowledge of risk management processes	
K0676	Know	Knowledge of cybersecurity laws and regulations	
K0677	Know	Knowledge of cybersecurity policies and procedures	
K0678	Know	Knowledge of privacy laws and regulations	
K0679	Know	Knowledge of privacy policies and procedures	
K0680	Know	Knowledge of cybersecurity principles and practices	
K0681	Know	Knowledge of privacy principles and practices	
K0682	Know	Knowledge of cybersecurity threats	
K0683	Know	Knowledge of cybersecurity vulnerabilities	
K0684	Know	Knowledge of cybersecurity threat characteristics	
K0685	Know	Knowledge of access control principles and practices	
K0686	Know	Knowledge of authentication and authorization tools and techniques	
K0688	Know	Knowledge of common application vulnerabilities	
K0698	Know	Knowledge of cryptographic key management principles and practices	
K0701	Know	Knowledge of data backup and recovery policies and procedures	
K0710	Know	Knowledge of enterprise cybersecurity architecture principles and practices	
K0716	Know	Knowledge of host access control (HAC) systems and software	
K0717	Know	Knowledge of network access control (NAC) systems and software	
K0728	Know	Knowledge of Confidentiality, Integrity and Availability (CIA) principles and practices	
K0729	Know	Knowledge of non-repudiation principles and practices	
K0730	Know	Knowledge of cyber safety principles and practices	
K0742	Know	Knowledge of identity and access management (IAM) principles and practices	
K0751	Know	Knowledge of system threats	
K0752	Know	Knowledge of system vulnerabilities	
K0760	Know	Knowledge of server diagnostic tools and techniques	
K0761	Know	Knowledge of Fault Detection and Diagnostics (FDD) tools and techniques	
K0770	Know	Knowledge of system administration principles and practices	
K0778	Know	Knowledge of enterprise information technology (IT) architecture principles and practices	
K0779	Know	Knowledge of systems engineering processes	
K0783	Know	Knowledge of network attack characteristics	
K0791	Know	Knowledge of defense-in-depth principles and practices	
K0797	Know	Knowledge of ethical hacking tools and techniques	
K0813	Know	Knowledge of interpreted and compiled programming language characteristics	
K0832	Know	Knowledge of cyberattack characteristics	
K0833	Know	Knowledge of cyberattack actor characteristics	
K0837	Know	Knowledge of hardening tools and techniques	
K0844	Know	Knowledge of cyber attack stages	
K0845	Know	Knowledge of cyber intrusion activity phases	
K0865	Know	Knowledge of data classification standards and best practices	
K0866	Know	Knowledge of data classification tools and techniques	
K0870	Know	Knowledge of enterprise architecture (EA) reference models and frameworks	
K0871	Know	Knowledge of enterprise architecture (EA) principles and practices	
K0879	Know	Knowledge of industry cybersecurity models and frameworks	
K0880	Know	Knowledge of access control models and frameworks	
K0882	Know	Knowledge of ethical hacking principles and practices	
K0891	Know	Knowledge of the Open Systems Interconnect (OSI) reference model	
K0915	Know	Knowledge of network architecture principles and practices	
K0924	Know	Knowledge of network analysis tools and techniques	
K0934	Know	Knowledge of data classification policies and procedures	
K0939	Know	Knowledge of packet-level analysis tools and techniques	
K0942	Know	Knowledge of cryptology principles and practices	
K0955	Know	Knowledge of penetration testing principles and practices	

TKS ID	Type	Description	New
K0956	Know	Knowledge of penetration testing tools and techniques	
K0969	Know	Knowledge of cyber-attack tools and techniques	
K0983	Know	Knowledge of computer networking principles and practices	
K1014	Know	Knowledge of network security principles and practices	
K1076	Know	Knowledge of risk scoring principles and practices	
K1079	Know	Knowledge of web application security risks	
K1087	Know	Knowledge of social engineering tools and techniques	
K1129	Know	Knowledge of cyber defense auditing laws and regulations	
K1130	Know	Knowledge of cyber defense auditing policies and practices	
K1182	Know	Knowledge of organizational cybersecurity policies and configurations	
S0483	Skil	Skill in identifying software communications vulnerabilities	
S0492	Skil	Skill in performing threat environment analysis	
S0532	Skil	Skill in analyzing software configurations	
S0543	Skil	Skill in scanning for vulnerabilities	
S0544	Skil	Skill in recognizing vulnerabilities	
S0572	Skil	Skill in detecting host- and network-based intrusions	
S0574	Skil	Skill in developing security system controls	
S0578	Skil	Skill in evaluating security designs	
S0588	Skil	Skill in performing threat modeling	
S0591	Skil	Skill in performing social engineering	
S0597	Skil	Skill in writing code in a currently supported programming language	
S0641	Skil	Skill in reviewing logs	
S0642	Skil	Skill in identifying evidence of past intrusions	
S0656	Skil	Skill in assessing application vulnerabilities	
S0675	Skil	Skill in optimizing system performance	
S0686	Skil	Skill in performing risk assessments	
S0688	Skil	Skill in performing network data analysis	
S0804	Skil	Skill in assessing an organization's threat environment	
T1020	Task	Determine the operational and safety impacts of cybersecurity lapses	
T1041	Task	Determine impact of software configurations	
T1069	Task	Evaluate organizational cybersecurity policy regulatory compliance	
T1070	Task	Evaluate organizational cybersecurity policy alignment with organizational directives	
T1079	Task	Develop cybersecurity risk profiles	
T1084	Task	Identify anomalous network activity	
T1091	Task	Perform authorized penetration testing on enterprise network assets	
T1118	Task	Identify vulnerabilities	
T1119	Task	Recommend vulnerability remediation strategies	
T1229	Task	Maintain deployable cyber defense audit toolkits	
T1279	Task	Prepare audit reports	
T1341	Task	Perform required reviews	
T1489	Task	Correlate incident data	
T1619	Task	Perform risk and vulnerability assessments	
T1620	Task	Recommend cost-effective security controls	