Developmental Test Cyber Vulnerability Analysis Standards

This document assists DoD and industry Test and Evaluation (T&E) professionals with identifying developmental T&E cybersecurity knowledge, skills, and abilities (KSAs) that may be included in a qualification process or program for organizational-level and/or analyst-level qualification standards. This document focuses on T&E cybersecurity KSAs common across all DoD components. Components, or organizations within these components, may have specific T&E guidance, operational processes, or procedures that each deems necessary for tailoring these standards through additional qualification KSAs.

Introduction

Developmental Test Cyber Vulnerability Analysis (DT Cyber VA) standards represent the baseline set of standards for organizations and analysts engaged in developmental T&E. These standards assess two key components:

1. Organizational standards assess whether DT Cyber VA organizations have the administrative capability to support events, are staffed with highly qualified cyber VA personnel, and are committed to the development and retention of their workforce.
2. Analyst standards assess the understanding and mastery of KSAs cybersecurity analysts are expected to possess for the execution of a DT cyber event.

Organizational standards provide assurance to the Program Executive Office (PEO) and Program Manager (PM) that organizations are equipped to conduct cybersecurity vulnerability assessments, while analyst standards provide assurance to the DoD component or organization that analysts are highly qualified to execute and participate in DT cyber events.

Two categories comprise Cyber VA standards: (1) Organizational Standards and (2) Cyber VA Analyst Standards. Cyber VA Analyst Standards include Cyber T&E Lead Standards at an advanced level with qualification standards specific to analyst leadership. The DoD Cybersecurity T&E Guidebook, version 2.0 (25 Apr 2018), also briefly describes both roles. These standards allow organizations to train and develop their workforce to adequately support the first four Cybersecurity T&E Phases as described in the DoD Cybersecurity T&E Guidebook. The phases, mapped to the acquisition lifecycle, are shown in Figure 1. Figure 1 represents the cybersecurity T&E phases where there is ample time in the life cycle for all phase activities and for a non-tailored acquisition life cycle. Some systems, however, enter the acquisition lifecycle at Milestone (MS) B, incrementally update major components of the system, are already well into the acquisition life cycle when cybersecurity T&E phases are initiated, or do not follow the traditional acquisition policy for other reasons. Accelerated acquisition programs may not have time for the full progression through the phases as depicted in Figure 1; however, the Cyber T&E Lead should support the program office in performing the early phases to establish the foundation for efficient cybersecurity and resilience testing.

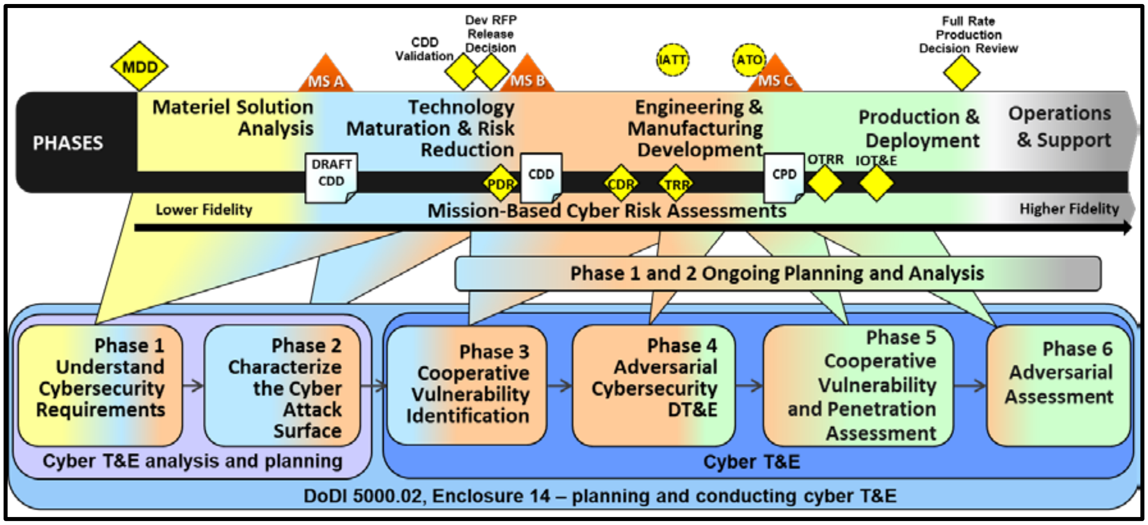
MDD
MS A
CDD Validation
Dev RFP Release Decision
MS B
IATT
ATO
MS C
Full Rate Production Decision Review
PHASES
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Production & Deployment
Operations & Support
DRAFT CDD
PDR
CDD
CDR
TRR
CPD
OTRR
IOT&E
Lower Fidelity
Mission-Based Cyber Risk Assessments
Higher Fidelity
Phase 1 and 2 Ongoing Planning and Analysis
Phase 1 Understand Cybersecurity Requirements
Phase 2 Characterize the Cyber Attack Surface
Phase 3 Cooperative Vulnerability Identification
Phase 4 Adversarial Cybersecurity DT&E
Phase 5 Cooperative Vulnerability and Penetration Assessment
Phase 6 Adversarial Assessment
Cyber T&E analysis and planning
Cyber T&E
DoDI 5000.02, Enclosure 14 – planning and conducting cyber T&E

Figure 1. Cybersecurity T&E Phases Mapped to the Acquisition Life Cycle

The remaining sections of this document outline the baseline DT Cyber VA standards required to support and execute DT Cyber VA events.

DT Cyber VA Organizational Standards

Organizational DT Cyber VA standards ensure organizations are equipped to conduct cyber vulnerability assessments and analyses across phase 1 to 4 of the Acquisition Cyber T&E Guidebook. DT Cyber VA organizations should have mechanisms in place that allow them to support cyber workforce professional development, laboratory and facilities to support training and workforce maturation, and production in support cyber VA (test plans, risk analysis methodologies, final report templates, and other processes and procedures that support DT Cyber VA events). Table 1 lists the baseline qualification standards to support Cyber T&E.

Table 1

DT Cyber VA Organization Qualification Standards

Organizational Capability	**Qualification Standards**
O1 - Professional Development	O1.1 – The organization possesses funding line to provide formal industry vendor training. O1.2 – The organization possesses capability to develop and maintain in-house training that is specialized and targeted to customer mission space. O1.3 – The organization possesses capacity for participation in R&D/S&T innovation projects to support cyber vulnerability analysis and assessments. O1.4 – The organization is an active participant in Joint cybersecurity VA training exercises. O1.5 – The organization provides cyber SME workforce career advancement opportunities for formal education, temporary assignment rotations, and DAU.

O2 – Cyber VA Tools	O2.1 – The organization possesses resources and capacity to develop custom mission-based cyber VA tools, techniques, and methodologies. O2.2 – The organization possesses configuration management processes, procedures, and infrastructure for cyber VA tools. O2.3 – The organization possesses appropriate documentation for the use of developed cyber VA tools such as an Acceptable Use Policy (AUP); defines rules and conditions for authorized use for cyber workforce with appropriate management signatures.
O3 – Laboratory and Facilities	O3.1 – The organization possesses laboratory facilities, environments, and infrastructure (i.e., virtual environment, capabilities, and appropriate classification-levels) aligned to customer and cyber T&E mission/technology to facilitate professional development. O3.2 – The organization possesses accredited procedures and facilities at the proper classification level for appropriate handling and safeguarding of classified storage and email access. O3.3 – The organization possesses range connectivity to include NCRC (JMN/JIOR).
O4 – Human Capital	O4.1 – The organization possesses processes and procedures, as part of their hiring plan, to hire qualified cyber SMEs who have appropriate clearances. O4.2 – The organization provides opportunities to incentivize and retain cyber workforce.
O5 – Procurement	O5.1 – The organization possesses funding line to procure equipment and services to support cyber T&E.
O6 – Work Products Standards (Test Plan)	O6.1 – The organization possesses capacity to staff test plans in support of Cyber VA events. Outline and sections of test plans should include (but not limited to): 1. Rules of Engagement (ROE)/Ground Rules (may not be included in the test plan, but accompany it) 2. Cyber VA Methodology / Cyber VA Tools 3. System Characterization to include system mission, authorization boundary, data flows, maintenance/supply-chain, cyber resilience capabilities and deployed countermeasures 4. Characterized Attack Cyber-Attack surface and Attack Vectors 5. Cyber VA event constraints and identified limitations
O7 – Work Product Standards (Final Report)	O7.1 – The organization possesses capacity to staff Cyber VA technical reports. Outline and sections of technical reports should include (but not limited to): 1. Evidence of confirmed cyber vulnerabilities to include cyber kill chain analysis

	2. Cyber VA Risk Assessment 3. Mitigation / Risk Management recommendations
O8 – Legal Review Process	O8.1 – The organization possesses internal legal review process to cover: 1. Approval of all standard (template) test plans, SOPs, ROEs. 2. Response to test critical questions or issues within 48 hours for any Cyber VA event.
O9 – Threat Intel Community Relationship	O9.1 – The organization possesses established relationships with the Threat intelligence community to include: 1. An established linkage and relationship with an organization that provides threat intelligence information that is directly related to the Cyber VA space that the organization executes in (e.g. CANBUS threats, networking threats, Linux or Windows threats, etc) 2. Participation in meetings and working groups for information sharing sessions with an established threat intelligence organization no less than 2 times per year with the objective of gaining knowledge and insight into foreign threats against the systems the organization tests.
O10 – Standard Operating Procedures	O10.1 – The organization possesses a baseline set of standard operating procedures (SOPs) in support of cyber T&E that ensure the organization conducts effective planning, execution, and post-analysis of cyber VA events, to include: 1. Cyber VA Tools Acceptable Use Policy. 2. Emergency Halting Procedures. 3. Open Network Notification Procedures. 4. Physical and Electronic Protection Policies & Procedures. 5. Material Handling and Destruction Procedures. 6. Client Data Protection Procedures. 7. Logging of Activities Policies & Procedures. 8. Sanitizing Client Information Systems. 9. ROE Template. 10. De-confliction Procedures for Cyber VA Teams during Cyber VA events. 11. Initiation & Handling of Customer Requests for Support. 12. Reporting of Daily, Weekly, Draft and Final Reports. 13. Roles and Responsibilities of Operators and Leads.

DT Cyber VA Analyst Standards

Competency Maturity

The DT Cyber VA standards use a Competency Maturity Model to measure and indicate a cybersecurity analyst capabilities and overall progress in the qualification process. Analysts are measured by their attained level of KSAs, including any other requirements mandated by the analyst's employer to include requisite security clearances. Figure 2 illustrates the process that analysts would follow to advance their qualifications and T&E career.

Analysts begin in the Apprentice Phase and advance to the Journeyman Phase by completing Apprentice Level Qualification Standards. Analysts in the Journeyman Phase advance to the Master Phase by completing Journeyman Level Qualification Standards. When progressing into the Master Phase, the structure of the qualification standards support specialization for either an Experienced Cybersecurity Analyst role or a Cyber T&E Lead role.

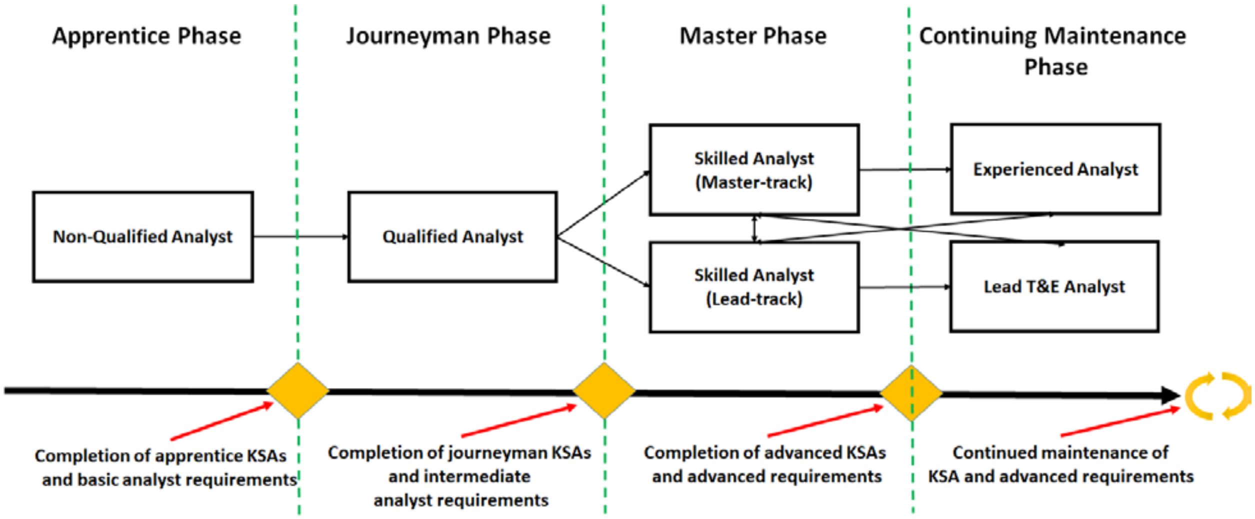
Apprentice Phase
Journeyman Phase
Master Phase
Continuing Maintenance Phase
Non-Qualified Analyst
Qualified Analyst
Skilled Analyst (Master-track)
Skilled Analyst (Lead-track)
Experienced Analyst
Lead T&E Analyst
Completion of apprentice KSAs and basic analyst requirements
Completion of journeyman KSAs and intermediate analyst requirements
Completion of advanced KSAs and advanced requirements
Continued maintenance of KSA and advanced requirements

Figure 2. DT Cyber VA Analyst Competency Maturity Model Phases

The next sections address progression between Competency Maturity Model Phases and the qualification standards for each phase.

Progression

Analysts often enter organizations as a Non-Qualified Cybersecurity Analyst. These analysts are considered to be in the Apprentice Phase. To assist analysts in progressing to the next phase of their qualifications, the standards specify the technical and non-technical KSAs required to advance to the Journeyman Phase. These KSAs are shown in Table 4. When an analyst enters an organization with existing qualifications, the gaining organization assesses the alignment of the analyst's qualifications to the Competency Maturity Model and may place the analyst in a role that is both suitable to the organization's needs and commensurate with the analyst's competency level.

An analyst in the Journeyman Phase is considered a Qualified Cybersecurity Analyst. Similar to the Apprentice Phase, an analyst in the Journeyman Phase must qualify on all Journeyman KSAs shown in Table 5, in addition to intermediate requirements specified by the organization, to proceed to the Master level.

An analyst in the Master Phase is considered a Skilled Cybersecurity Analyst. The standards specify two paths for qualification in the Master Phase. Completion of the Journeyman KSAs and analyst requirements allows an analyst to qualify for either a role of Cyber T&E Lead or an Experienced Cybersecurity Analyst. Role navigation may be dynamic, based on organizational requirements, event conditions, or by choice of the analyst. Analysts may first enter the Master Phase in the technical role of Experienced Cybersecurity Analyst, and later perform an intra-level movement into the Cyber T&E Lead leadership role. Role navigation is similar if the role of Cyber T&E Lead is taken on before becoming an Experienced Cybersecurity Analyst.

Once an analyst completes one of the two qualification standards in the Master Phase, the analysist is an Experienced Cybersecurity Analyst or a Lead T&E Cybersecurity Analyst, depending on the completed qualification. Upon completion of a qualification, analysts are responsible for performing continued maintenance of KSAs. Enforcement of continued maintenance of KSAs and advanced requirements at this level is the responsibility of the organization. At this point of an analyst’s development, areas of expertise become focused. More technical KSAs are expected for an Experienced Cybersecurity Analyst, while additional non-technical KSAs are expected for a Cyber T&E Lead. Technical requirements should be taken into consideration when developing additional KSAs for each role. The DT Cyber VA standards provides a set of advanced requirements only for the Cyber T&E Lead role. This information is shown in the following section. Similar to the consideration of additional KSAs, advanced requirements may be added to either role based on the needs of the organization. Table 3 shows how analyst are classified as they progress between phases.

Table 3

Summary of Analyst Qualification Progressions

If the analyst has completed the below phase…	**… they are classified as the following analyst …**	**… and are now working in the below phase.**
None	Non-Qualified Analyst	Apprentice
Apprentice	Qualified Analyst	Journeyman
Journeyman	Skilled Analyst	Master
Master (Master-track)	Experienced Analyst	Continuing Maintenance
Master (Lead-track)	Lead T&E Analyst	Continuing Maintenance

DT Cyber VA Organizations may specify additional KSAs, above and beyond the standardized DT Cyber VA KSAs, based on their internal needs. The organization must categorize supplemental KSAs under Apprentice, Journeyman, or Master Phases. The standardized DT Cyber VA KSAs represent the minimum standard for the DT Cyber VA workforce. Organizations may expand to define specialized KSAs, such as non-Internet Protocol or cyber-electronic warfare KSAs, but may not alter or reduce these minimum KSAs.

Apprentice Level Analysts Standards

Table 4

Apprentice Phase KSAs

Level	KSA Description	Source
A001	Ability to answer questions in a clear and concise manner.	NCWF A0011
A002	Knowledge of cryptography and cryptographic key management concepts.	NCWF K0019
A003	Basic knowledge of packet-level analysis.	NCWF K0062
A004	Basic knowledge of query languages such as SQL (structured query language).	NCWF K0069
A005	Knowledge of basic concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	NCWF K0108
A006	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	NCWF K0117
A007	Knowledge of virtualization technologies and virtual machine development and maintenance.	NCWF K0130
A008	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).	NCWF K0158
A009	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	NCWF K0179
A010	Knowledge of ethical hacking principles and techniques.	NCWF K0206
A011	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	NCWF K0362
A012	Knowledge of basic wireless applications, including vulnerabilities in various types of wireless applications.	NCWF K0375
A013	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	NCWF K0516
A014	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).	NCWF K0536
A015	Knowledge of the ways in which targets or threats use the Internet.	NCWF K0603
A016	Skill in diagnosing connectivity problems.	NCWF S0033
A017	Skill in using virtual machines.	NCWF S0073
A018	Skill in researching essential information.	NCWF S0268

A019	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.	NCWF S0289
A020	Skill in utilizing network analysis tools to identify software communications vulnerabilities, such as the use of clear text protocols to transfer sensitive information or credentials and the transmission of unknown, unexpected, or unauthorized network traffic.	NICE KSA 1067
A021	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks), and one or more tools and techniques that may be used in each stage.	NICE KSA 1069
A022	Knowledge to describe the basic types of encryption methodologies, terms used in each, and how each are generally used.	NICE KSA 1114
A023	Knowledge of system and application security threats and vulnerabilities.	NICE KSA 123
A024	Knowledge of routine Windows systems administration concepts, tasks, and terms.	NICE KSA 127
A025	Knowledge of the types of Intrusion Detection System (IDS) hardware and software.	NICE KSA 146
A026	Skill in network mapping, recreating simple network topologies, and enumerating open ports.	NICE KSA 212
A027	Knowledge of the differences between Type 1, 2, 3 and 4 encryption.	NICE KSA 27
A028	Knowledge of the use of common network tools (e.g., ping, traceroute, nslookup, arp) and how to interpret the information results.	NICE KSA 271
A029	Skill in using ACAS (Nessus and Security Center) and other vulnerability scanners against DoD/DoN Information Systems and PIT systems.	NICE KSA 3
A030	Knowledge of database management systems, query languages, table relationships, and views, and how they are used to create a functional database.	NICE KSA 32
A031	Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).	NICE KSA 342
A032	Knowledge of MS Windows command line (e.g., ipconfig, netstat, dir, nbtstat) and their functions.	NICE KSA 347
A033	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	NICE KSA 364
A034	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, Visual Basic Scripting [VBS]) on Windows and Unix systems (e.g., tasks such as parsing large data files, automating manual tasks, fetching/processing remote data).	NICE KSA 371

A035	Ability to correctly locate vulnerable applications or systems based on the output of automated vulnerability scan reports.	NICE KSA 4
A036	Knowledge of basic facts and terms used to describe host and network access control mechanisms (e.g., access control list).	NICE KSA 49
A037	Knowledge of network design processes, including security objectives, operational objectives, and tradeoffs.	NICE KSA 82
A038	Knowledge of which protocols are used in traffic flows across the network at each level of the OSI model.	NICE KSA 92
A039	Knowledge of the types of security event correlation tools.	NICE KSA 923
A040	Knowledge of deconfliction processes and procedures.	NCWF K0422
A041	Skill in preparing and presenting briefings.	NCWF S0249
A042	Skill in preparing plans and related correspondence.	NCWF S0250
A043	Skill in technical writing.	NCWF S0281
A044	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	NCWF S0356
A045	Knowledge of the facts, terms, and principles associated with well-known application vulnerabilities (to include web and mobile applications), as well as common "Top 20" security lists (SANS, OWASP, etc) describing vulnerabilities and countermeasures.	NICE KSA 10
A046	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	NICE KSA 58
A047	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored]) and the intent, capabilities, and opportunities of each in relation to a specific Information System or PIT system	NICE KSA 992
A048	Knowledge of the terms and concepts used in risk and threat assessment.	NICE KSA 1021
A049	Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.	NICE KSA 1126
A050	Knowledge of the Security Assessment and Authorization (SA&A) process.	NICE KSA 53
A051	Knowledge of the facts, terms, and concepts used in DoD cyber defense policies, procedures, and regulations.	NICE KSA 984
A052	Knowledge of common tactics, techniques, and procedures (TTPs) that second and third generation	NICE KSA 991

	threat actors may use to execute different classes of network attacks (e.g., passive, active, insider, close-in, and distribution) on Department of Defense / Department of Navy networks.	
A053	Knowledge of general Supervisory control and data acquisition (SCADA) system components.	NICE KSA 0437
A054	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	NICE KSA 0137
A055	Knowledge of common non Internet Protocol (Non-IP) data transmission systems used within the military by vehicles and aircrafts (1553, CAN, etc.).	Cyber VA DT XSWG

Journeyman Level Analyst Standards

Table 5

Journeyman Phase KSAs

Level	KSA Description	Source
J001	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	NCWF A0089
J002	Ability to identify/describe target vulnerability.	NCWF A0092
J003	Ability to identify/describe techniques/methods for conducting technical exploitation of the target.	NCWF A0093
J004	Knowledge of covert communication techniques.	NCWF K0209
J005	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	NCWF K0296
J006	Knowledge of encryption algorithms, stenography, and other forms of data concealment.	NCWF K0305
J007	Knowledge of embedded systems.	NCWF K0322
J008	Knowledge of basic wireless applications, including vulnerabilities in various types of wireless applications.	NCWF K0386
J009	Knowledge of denial and deception techniques.	NCWF K0424
J010	Knowledge of encryption algorithms and tools for WLANs.	NCWF K0428
J011	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.	NCWF K0469
J012	Knowledge of system administration concepts for the Unix/Linux and Windows operating systems (e.g., process management, directory structure, installed applications, Access Controls).	NCWF K0537
J013	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	NCWF K0608
J014	Skill in analyzing memory dumps to extract information.	NCWF S0062
J015	Skill in preparing Test & Evaluation reports.	NCWF S0115
J016	Skill in writing scripts using R, Python, PIG, HIVE, SQL, etc.	NCWF S0130
J017	Skill in analyzing essential network data (e.g., router configuration files, routing protocols).	NCWF S0178
J018	Skill in processing collected data for follow-on analysis.	NCWF S0252

J019	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).	NCWF S0257
J020	Skill in remote command line and Graphic User Interface (GUI) tool usage.	NCWF S0267
J021	Skill in writing effective reports.	NCWF S0302
J022	Skill in analyzing a target's communication networks.	NCWF SO177
J023	Skill in correlating the output of vulnerability scanning tools, debuggers, fuzzers, compliance tools, Group Policy Object reports, and/or network analysis tools to identify and validate system and network vulnerabilities and to create accurate, custom vulnerability reports and POA&Ms.	NICE KSA 3
J024	Ability to use data from a wide variety of sources, automated and manual, to identify the root cause of specific weaknesses in the security posture of a target Information System, PIT system, IT Service, or IT Product due to technical, organizational, or programmatic issues, and provide specific recommendations to manage the risk.	NICE KSA 4
J025	Knowledge of Unix/Linux operating system structure and internals (e.g., process management, directory structure, installed applications).	NICE KSA 1063
J026	Skill in utilizing a mix of vulnerability scanning and exploitation tools (e.g., fuzzers, packet sniffers, debuggers) to identify system/software vulnerabilities (e.g., penetration and testing).	NICE KSA 1066
J027	Knowledge of reverse engineering concepts.	NICE KSA 1089
J028	Knowledge of anti-virus evasion and anti-forensics tools, techniques, and procedures (TTPs) and how they may be applied to maintain persistence or otherwise cover an attacker's tracks in UNIX and Windows environments.	NICE KSA 1092
J029	Knowledge of software debugging principles.	NICE KSA 116
J030	Skill in applying host/network access controls (e.g., access control list).	NICE KSA 157
J031	Skill in configuring and properly employing common open source tools (e.g. Metasploit Framework, MimiKatz PowerShell Empire) to mimic threat behaviors.	NICE KSA 210

J032	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump) in order to identify specific information within network packets indicating anomalous or malicious behavior within network traffic flows.	NICE KSA 214
J033	Skill in one or more of the following disciplines in order to gain access to a network, system, or sensitive data: social engineering techniques; web application penetration testing, wireless penetration testing, ICS, non-IP based, RF, virtual, close access testing, etc.	NICE KSA 226
J034	Knowledge of computer programming principles in order to state the differences between object-oriented programming, procedural programming, and functional programming and select an appropriate use and language for each.	NICE KSA 23
J035	Knowledge of the principles and uses of widely-deployed encryption algorithms and how they are used (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange[IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	NICE KSA 25
J036	Knowledge of common adversary tactics, techniques, and procedures (TTPs) in assigned area of responsibility (e.g., historical country-specific TTPs, emerging capabilities).	NICE KSA 270
J037	Knowledge of the principles of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools to protect data and critical operations.	NICE KSA 29
J038	Knowledge of hacking methodologies and tools commonly used to exploit well-known vulnerabilities in the Windows or Unix/Linux environment.	NICE KSA 294
J039	Skill in building, updating, and executing ACAS and other vulnerability scanning and compliance checking tools (Security Content Automation Protocol (SCAP) Compliance Checker [SCC], HBSS Policy Auditor, Windows Secure Update Services, etc.) to accurately and consistently capture network vulnerability scans and create automated reports for the purposes of compliance reporting.	NICE KSA 3
J040	Skill in techniques and tools to identify and assess common vulnerabilities found in databases and to recommend mitigation strategies to address identified weaknesses.	NICE KSA 34

J041	Knowledge of which system files (e.g., log files, registry files, and configuration files) contain relevant information (system enumeration, data exfiltration) and where to find those system files.	NICE KSA 346
J042	Ability to identify and draw general conclusions regarding programmatic, design, and /or operational security issues based on results of vulnerability scans, compliance checks, and other configuration data (GPOs, WSUS, etc).	NICE KSA 4
J043	Ability to use vulnerability scans, compliance checks, and other configuration data (GPOs, WSUS, etc) to accurately identify specific inconsistencies within system documentation (vendor claims, DIACAP/RMF artifacts, CONOPS, systems engineering plans, design specifications, interface descriptions, etc) and the actual applied security controls as developed or deployed within an Information System, PIT system, IT product, or provided in IT services.	NICE KSA 4
J044	Knowledge of the principles used in intrusion detection methodologies and the techniques used for detecting host-and network-based intrusions through intrusion detection technologies.	NICE KSA 66
J045	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	NICE KSA 895
J046	Knowledge of syntax of two or more compiled and interpreted languages in order to accurately determine the function of specific code in a program and successfully modify the code to tailor all or portions of the program to a specific need.	NICE KSA 904
J047	Knowledge of common attack vectors for layers 1-4 (OSI Model), to include wireless attack vectors and the tools and techniques commonly used to exploit network devices.	NICE KSA 990
J048	Knowledge of common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, mail, Domain Name System [DNS]) and how they interact to provide network communications in order to successfully design, integrate, troubleshoot, or assess the deployment of cybersecurity tools into the network.	NISE KSA 139
J049	Knowledge of the characteristics of physical and virtual data storage media.	NCWF K0097
J050	Knowledge of all relevant reporting and dissemination procedures.	NCWF K0354

J051	Knowledge of both internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.	NCWF K0376
J052	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	NCWF K0379
J053	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.	NCWF K0508
J054	Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.	NCWF K0509
J055	Knowledge of organizational and partner policies, tools, capabilities, and procedures.	NCWF K0510
J056	Knowledge of strategies and tools for target research.	NCWF K0535
J057	Skill in conducting test events.	NCWF S0015
J058	Skill in writing test plans.	NCWF S0061
J059	Skill in identifying gaps in technical capabilities.	NCWF S0066
J060	Skill in writing (and submitting) requirements to meet gaps in technical capabilities.	NCWF S0300
J061	Knowledge of relevant laws, policies, procedures, or governance related to work impacting critical infrastructure.	NICE KSA 1040
J062	Skill in developing operations-based testing scenarios.	NICE KSA 176
J063	Knowledge of methods to identify critical system components, data, and information flows, and to develop effective plans to assure their availability and/or minimize service outage in the event of an adverse system event.	NICE KSA 37
J064	Knowledge of a DoD program's or organization's risk tolerance and/or risk management approach.	NICE KSA 965
J065	Skill in safe test and evaluation techniques for Industrial Control Systems (ICS) consisting of installations and deployable platforms such as ships and aircraft.	Cyber VA DT XSWG
J064	Skill in conducting cyber-attacks via code and data injections within unsecure Non-IP data communications protocols (1553, CAN, etc.).	Cyber VA DT XSWG

J065	Knowledge of supply chain risks on how adversaries may introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system.	DoD Cyber Table Top Guidebook, V1

Master Level Analyst Standards (Experienced Cybersecurity Analyst)

Table 6

Master Phase KSAs for Experienced Cybersecurity Analyst

Level	KSA Description	Source
M001	Ability to collect, verify, and validate test data.	NCWF A0030
M002	Ability to translate data and test results into evaluative conclusions.	NCWF A0040
M003	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	NCWF A0075
M004	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	NCWF K0181
M005	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	NCWF K0188
M006	Knowledge of multi-level/security cross domain solutions.	NCWF K0240
M007	Knowledge of sustainment technologies, processes and strategies.	NCWF K0249
M008	Knowledge of how modern wireless communications systems impact cyber operations.	NCWF K0446
M009	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	NCWF K0614
M010	Skill in maintaining databases.	NCWF S0042
M011	Skill in maintaining directory services.	NCWF S0043
M012	Advanced skills in the use of tools and techniques in two or more of the following penetration testing disciplines in order to gain access to a network, system, or sensitive data: social engineering techniques; web application penetration testing, wireless penetration testing, ICS, non-IP based, RF, virtual, close access testing, mobile device penetration testing, etc.	NCWF S0051
M013	Skill in assessing the application of cryptographic standards.	NCWF S0164
M014	Skill in analyzing target communications internals and externals collected from wireless LANs.	NCWF S0182
M015	Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings	NCWF S0270

	analysis) to identify function and ownership of remote tools.	
M016	Skill in testing and evaluating tools for implementation.	NCWF S0282
M017	Skill in wireless network target analysis, templating, and geolocation.	NCWF S0299
M018	Knowledge of programming language structures (to include complex data structures) and logic used in compiled and interpreted languages.	NICE KSA 102
M019	Advanced knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code) and the tools and techniques to discover and exploit Zero Day system and application vulnerabilities.	NICE KSA 105
M020	Skill in using and identifying obfuscation techniques.	NICE KSA 1100
M021	Skill in privilege escalation and maintaining persistence on a compromised system.	NICE KSA 225
M022	Knowledge of the capabilities, configuration options, benefits, hardware requirements, and shortcomings of specific vendor and open source ID/PS solutions and event correlation tools widely used within DoD and DoN networks.	NICE KSA 59
M023	Knowledge of low-level computer languages (e.g., assembly languages), to include mnemonics and how the different types of instructions and memory declarations are used.	NICE KSA 74
M024	Skill in using packet crafting tools and packet-level analysis tools to craft, record, and replay network traffic flows.	NICE KSA 922
M025	Skill in analyzing anomalous code as malicious or benign.	NICE KSA 1098
M026	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures (TTP).	NICE KSA 1101
M027	Skill in conducting software debugging.	NICE KSA 168

Master Level Analyst Standards (Cyber T&E Lead Analyst)

Table 7

Master Phase KSAs for Cyber T&E Lead Analyst

Level	KSA Description	Source
L001	Ability to develop or recommend analytic approaches or solutions to problems and situations for which no precedent exists.	NCWF A0080
L002	Ability to develop, update, and/or maintain standard operating procedures (SOPs).	NCWF A0034
L003	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.	NCWF A0116
L004	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber-attack) principles, capabilities, limitations, and effects.	NCWF K0408
L005	Knowledge of organization objectives, leadership priorities, and decision-making risks.	NCWF K0506
L006	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.	NCWF S0112
L007	Skill in providing Test & Evaluation resource estimate.	NCWF S0117
L008	Skill in performing impact/risk assessments.	NCWF S0171
L009	Skill in creating plans in support of remote operations.	NCWF S0201
L010	Skill in generating operation plans in support of mission and target requirements.	NCWF S0223
L011	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.	NCWF S0309
L012	Knowledge of the capabilities, configuration options, benefits, hardware requirements, and shortcomings of specific vendor and open source ID/PS solutions and event correlation tools widely used within DoD and DoN networks.	NICE KSA 59
L013	Skill in selecting the appropriate toolsets to assess the robustness of security systems and designs based on claims, specifications, and/or parameters stated in system documentation.	NICE KSA 160
L014	Skill in competently coordinating test activities amongst a team as well as using techniques and tools to capture, archive, compile and assess accuracy of test results from each team member.	NICE KSA 169
L015	Skill in determining an appropriate level of test rigor for a given system.	NICE KSA 182

L016	Skill in evaluating test plans for applicability and completeness.	NICE KSA 950
L017	Knowledge of local specialized system requirements (e.g., critical infrastructure systems) that may not use standard information technology [IT]) for safety, performance, and reliability, and the relationship of these requirements to law, regulations, and policies.	NISE KSA 1038
L018	Ability to analyze and assess available system/platform documentation to identify and define the cyber landscape.	2018 Cyber DT VA XSWG
L019	Ability to develop test plans for a system/event.	2018 Cyber DT VA XSWG
L020	Knowledge to describe and discuss the role of the Chief Development Officer/Tester in creating and developing test plans.	2018 Cyber DT VA XSWG
L021	Ability to, through analysis of the cyber landscape for the platform/system, identify threat vectors for the platform/system.	2018 Cyber DT VA XSWG
L022	Using identified threat vectors, the analyst can discuss possible impact to the mission of the platform/system.	2018 Cyber DT VA XSWG
L023	Ability to create a document defining and discussing the scope, requirements, limitations, and classification for a test event on the platform/system.	2018 Cyber DT VA XSWG
L024	Ability to, in cooperation with the platform/system owner/customer, develop and present rules of engagement (RoE) for a test event on the platform/system.	2018 Cyber DT VA XSWG
L025	Ability to understand and discuss the role of the platform/system customer and owner in developing test documentation.	2018 Cyber DT VA XSWG
L026	Ability to understand, read, and present system design and architecture diagrams, documents, figures, and artifacts.	2018 Cyber DT VA XSWG
L027	Ability to use system design and architecture artifacts to identify and characterize cyber threats, attack paths, and surfaces areas specific to the platform/system under test.	2018 Cyber DT VA XSWG
L028	Ability to analyze platform/system documentation, test plans, and other relevant platform/system documentation to create resources estimates including, but not limited to, event cost, OT, resources, and ROM.	2018 Cyber DT VA XSWG
L029	Ability to analyze platform/system documentation, test plans, and other relevant platform/system documentation to identify necessary capabilities and abilities for executing a	2018 Cyber DT VA XSWG

	test event, and can identify other analysts with aligned, complementary, or supporting skillsets.	
L030	Ability to describe the purpose and role of a security classification guide (SCG) in all aspects of the platform/system test event.	2018 Cyber DT VA XSWG
L031	Ability to apply other methods of derivative classification when no SCG is present and can identify the role and function of other individuals in assisting with this classification.	2018 Cyber DT VA XSWG
L032	Ability to create budgets for, coordinate resources, and complete the logistics for team travel, equipment allocation, and necessary shipping for a platform/system test event.	2018 Cyber DT VA XSWG
L033	Ability to describe and discuss the process for procure resources required for a test event and, if required, the process for seeking support from outside organizations.	2018 Cyber DT VA XSWG
L034	Ability to understand the role of intelligence in test event planning, can read and understand an intelligence report, and can discuss and describe how to apply this to test event planning.	2018 Cyber DT VA XSWG
L035	Ability to create and maintain efficient and easily accessible communication channels between team members.	2018 Cyber DT VA XSWG
L036	Ability to identify sources of policies and procedures for conducting test events, and can describe situations where stakeholder is approval is required.	2018 Cyber DT VA XSWG
L036	Ability to describe and discuss their role and contributions to Cyber T&E planning.	2018 Cyber DT VA XSWG
L037	Ability to understand the role, purpose, and function of the test event in-brief.	2018 Cyber DT VA XSWG
L038	Skill in preparing and delivering an in-brief for a test event.	2018 Cyber DT VA XSWG
L039	Ability to understand the role, purpose, and function of daily hot washes for test events.	2018 Cyber DT VA XSWG
L040	Skill in preparing and delivering a daily host-wash for a test event.	2018 Cyber DT VA XSWG
L041	Ability to understand the role, purpose, and function of an emergent results brief for test events.	2018 Cyber DT VA XSWG
L042	Skill in preparing and delivering an emergent results brief for a test event.	2018 Cyber DT VA XSWG
L043	Skill in describing the role that the rules of engagement and the test plan play in executing a test event, and can discuss how these are used to ensure an acceptable execution of a test event.	2018 Cyber DT VA XSWG
L044	Skill in describing the policy, procedure, and process for deviating from the test plan.	2018 Cyber DT VA XSWG

L045	Skill in describing the policy, procedure, and process for modifying the rules of engagement.	2018 Cyber DT VA XSWG
L046	Skill in describing and discussing their methodology for assigning tasks to team members, including why they find this method beneficial.	2018 Cyber DT VA XSWG
L047	Skill in describing and discussing their methodology for managing team members, including why they find this method beneficial.	2018 Cyber DT VA XSWG
L048	Skill in explaining the responsibilities of the team, and the lead analyst, for safeguarding classified information, to include policies, procedures, and processes for reporting suspected spillage.	2018 Cyber DT VA XSWG
L049	Skill in identifying, describing, and discussing organizational policies, procedures, and processes for safeguarding and managing test event data after an event.	2018 Cyber DT VA XSWG
L050	Skill in understanding the role, purpose, and function of after actions reviews (AAR) post-test event.	2018 Cyber DT VA XSWG
L051	Skill in preparing and conducting an after action review for an event.	2018 Cyber DT VA XSWG
L052	Skill in describing, in detail, their organizational process for analyzing event findings, to include: (1) addressing and assessing customer input, (2) assessing risk, (3) translating findings to an impact, (4) translating risk and impact to a mission impact.	2018 Cyber DT VA XSWG
L053	Skill in describing their organizational process for producing reports (and all other deliverables) to their customers.	2018 Cyber DT VA XSWG
L054	Skill in understanding and explaining their role, and the importance of, their final review of a report or any other publication.	2018 Cyber DT VA XSWG
L055	Skill in describing, in detail, their organizational process for formally publishing a report.	2018 Cyber DT VA XSWG
L056	Skill in understanding the role, purpose, and function of post-event briefs to the customer.	2018 Cyber DT VA XSWG
L057	Skill in preparing and delivering a post-event brief to a customer.	2018 Cyber DT VA XSWG
L058	Skill in understanding the role, purpose, and function of back-briefs for their cyber analysis team.	2018 Cyber DT VA XSWG
L059	Skill in preparing and delivering a back-brief to the cyber analysis team.	2018 Cyber DT VA XSWG
L060	Skill in describing the role, purpose, and function of tech-on-tech discussions, including organizational-specific options available to the customer.	2018 Cyber DT VA XSWG

L061	Skill in describing the role, purpose, and function of a verification of fixes, including organizational-specific options available to the customer.	2018 Cyber DT VA XSWG
L062	Ability to analyze and assess Program Protection Plans, Critical Analysis studies to include Supply Chain Risk Management artifacts of IP and Non-IP devices.	2018 Cyber DT VA XSWG
L063	Knowledge of supply chain threat assessments (software, hardware, firmware, embedded systems) and adverse impacts they system behavior.	The DoD Cyber Table Top Guidebook, V1
L064	Knowledge of software exploitation of vulnerabilities in components, sub-components, and maintenance support devices (MSD) and maintenance support equipment (MSE) systems.	The DoD Cyber Table Top Guidebook, V1
L065	Knowledge of military supply chain management utilized for integrating acquisition, supply, maintenance, and transportation functions with the physical, financial, information, and communications networks to satisfy joint force materiel requirements.	The DoD Cyber Table Top Guidebook, V1
L066	Knowledge of supply chain attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.	DoD Cyber Table Top Guidebook, V1
L067	Ability to plan, participate, and facilitate mission-based critical risk analyses (MBCRA)/cyber table top exercise (CTTX) to analyze system's attack surface in order to assess mission impact on suspected cyber vulnerabilities.	DoD Cyber T&E Guidebook