CAREER PATHWAY CYBER CRIME INVESTIGATOR (221)

November 2020

Developed By:

The Interagency Federal Cyber Career Pathways Working Group

Endorsed By:

Table of Contents

1 221-CYBER CRIME INVESTIGATOR

1.1 WORK ROLE OVERVIEW

The table below provides an overview of various role-specific elements related to 221-Cyber Crime Investigator.

Table 1. 221-Cyber Crime Investigator

NICE Role Description	*Identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.*
OPM Occupational Series	Personnel performing the 221-Cyber Crime Investigator work role are most commonly aligned to the following Occupational Series: (Top 5 Shown) - 1811-Criminal Investigation – 94% - 1801-General Inspection, Investigation, Enforcement, and Compliance – 2% - 2210-Information Technology – 2% - 1805-Investigative Analysis – <1% - 401-General Natural Resources Management and Biological Sciences – <1%
Work Role Pairings	Personnel performing the 221-Cyber Crime Investigator work role are most commonly paired with the following complimentary Work Roles (Top 5 shown): - 132-Target Network Analyst – 98% - 211-Forensics Analyst – <1% - 712-Cyber Instructor – <1% - 111-All-Source Analyst – <1% - 112-Mission Assessment Specialist – <1%
Functional Titles	Personnel performing the 221-Cyber Crime Investigator work role may unofficially or alternatively be called: - Computer Crime Investigator - Cyber Incident Handler / Responder - Special Agent
Distribution of GS-Levels	Personnel performing the 221-Cyber Crime Investigator work role are most commonly found within the following grades on the General Schedule.* - ☐ GS-3 – redacted** - ☐ GS-4 – redacted** - ☐ GS-5 – redacted** - ☐ GS-7 – redacted** - ☐ GS-8 – redacted** - ☒ GS-9 – 3%

	- ☒ GS-10 – 9% - ☒ GS-11 – 7% - ☒ GS-12 – 11% - ☒ GS-13 – 66% - ☐ GS-14 – redacted* - ☐ GS-15 – redacted* *.5% of all 221s are in non-GS pay plans and excluded from this section **Percentages less than 3% have been redacted
On Ramps	The following work roles are examples of possible roles an individual may perform prior to transitioning into the 221-Cyber Crime Investigator work role: - 211-Law Enforcement/Counterintelligence Forensics Analyst - 212-Cyber Defense Forensics Analyst - 531-Cyber Defense Incident Responder
Off Ramps	The following work roles are examples of possible roles an individual may transition to after having performed the 221-Cyber Crime Investigator work role: - 212-Cyber Defense Forensics Analyst - 211-Law Enforcement/Counterintelligence Forensics Analyst *Note: Leveraging the knowledge, skills, abilities, and tasks of the 411-Technical Support Specialist work role, individuals may prepare themselves to transition into one or more of the following cross-functional work roles: - *711- Cyber Instructional Curriculum Developer* - *712-Cyber Instructor* - *751-Cyber Workforce Developer and Manager* - *752-Cyber Policy and Strategy Planner* - *802-IT Project Manager*

1.2 CORE TASKS

The table below provides a list of tasks that represent the Core, or baseline, expectations for performance in the 221-Cyber Crime Investigator work role, as well as additional tasks that those in this role may be expected to perform.

Table 2. 221-Cyber Crime Investigator Core Tasks

Task ID	Task Description	Core or Additional
T0423	Analyze computer-generated threats for counterintelligence or criminal activity.	Core
T0433	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Core
T0103	Examine recovered data for information of relevance to the issue at hand.	Core
T0430	Gather and preserve evidence used on the prosecution of computer crimes.	Core
T0112	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Core
T0114	Identify elements of proof of the crime.	Core
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Core
T0343	Analyze the crisis situation to ensure public, personal, and resource protection.	Additional
T0346	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.	Additional
T0031	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Additional
T0453	Determine and develop leads and identify sources of information in order to identify and/or prosecute the responsible parties to an intrusion or other crimes.	Additional
T0360	Determine the extent of threats and recommend courses of action and countermeasures to mitigate risks.	Additional
T0059	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet.	Additional
T0471	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Additional
T0479	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.	Additional
T0096	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals).	Additional
T0104	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Additional
T0110	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Additional
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Additional

Task ID	Task Description	Core or Additional
T0120	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Additional
T0523	Prepare reports to document the investigation following legal standards and requirements.	Additional
T0386	Provide criminal investigative support to trial counsel during the judicial process.	Additional
T0225	Secure the electronic device or information source.	Additional
T0193	Process crime scenes.	Additional

1.3 CORE KNOWLEDGE, SKILLS, AND ABILITIES

The table below provides a ranking of KSAs that represent the Core, or baseline, expectations for performance in the 221-Cyber Crime Investigator work role, as well as additional KSAs that those in this role may be expected to demonstrate.

Table 3. 221-Cyber Crime Investigator Core KSAs

KSA ID	Description	Competency	Importance to Work Role
K0004	Knowledge of cybersecurity principles.	Information Systems/Network Security	Foundational to all work roles.
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	Infrastructure Design	Foundational to all work roles.
K0003	Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	Legal, Government, and Jurisprudence	Foundational to all work roles.
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	Risk Management	Foundational to all work roles.
K0005	Knowledge of cyber threats and vulnerabilities.	Vulnerabilities Assessment	Foundational to all work roles.
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	Vulnerabilities Assessment	Foundational to all work roles.
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics	Core
K0128	Knowledge of types and collection of persistent data.	Computer Forensics	Core
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics	Core
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics	Core
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design	Core
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence	Core

KSA ID	Description	Competency	Importance to Work Role
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics	Additional
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense	Additional
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense	Additional
S0072	Skill in using scientific rules and methods to solve problems.	Data Analysis	Additional
K0231	Knowledge of crisis management protocols, processes, and techniques.	Incident Management	Additional
K0209	Knowledge of covert communication techniques.	Intelligence Analysis	Additional
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence	Additional
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence	Additional
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence	Additional
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence	Additional
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence	Additional
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence	Additional
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	Third Party Oversight/Acquisition Management	Additional
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis	Additional
K0144	Knowledge of social dynamics of computer attackers in a global context.	Threat Analysis	Additional
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.	Threat Analysis	Additional
K0070	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).	Vulnerabilities Assessment	Additional

KSA ID	Description	Competency	Importance to Work Role
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment	Additional
A0174	Ability to find and navigate the dark web using the TOR network to locate markets and forums.	Web Technology	Additional

1.4 CORE COMPETENCIES

The table below is a compilation of competencies aligned to the 221-Cyber Crime Investigator work role, and their associated importance. Listed competencies are collections of three or more similar Knowledge, Skills, or Abilities aligned to the Work Role. *These competencies originate from the NICE Framework Competency Pivot Tool.*

Table 4. 221-Cyber Crime Investigator Core Competencies

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Legal, Government, and Jurisprudence	C030	KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.	• Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy. (K0003) • Knowledge of legal governance related to admissibility (e.g. Rules of Evidence). (K0123) • Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody. (K0125) • Knowledge of electronic evidence law. (K0155) • Knowledge of legal rules of evidence and court procedure. (K0156) • Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures. (K0168) • Knowledge of the judicial process, including the presentation of facts and evidence. (K0251) • Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation. (K0351)	Core
Computer Forensics	C005	KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.	• Knowledge of processes for seizing and preserving digital evidence. (K0118) • Knowledge of types and collection of persistent data. (K0128) • Skill in preserving evidence integrity according to standard operating procedures or national standards. (S0047) • Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data. (S0068) • Ability to examine digital media on multiple operating system platforms. (A0175)	Core

Technical Competency	Comp. ID	Definition	Work Role Related KSAs	Importance
Vulnerabilities Assessment	C057	KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.	• Knowledge of cyber threats and vulnerabilities. (K0005) • Knowledge of specific operational impacts of cybersecurity lapses. (K0006) • 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). (K0070) • Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list) (K0624)	Core
Threat Analysis	C055	KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.	• Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations. (K0107) • Knowledge of social dynamics of computer attackers in a global context. (K0144) • Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity. (K0244)	Additional

1.5 SUGGESTED QUALIFICATIONS / CAPABILITY INDICATORS

Table 5. 221-Cyber Crime Investigator Suggested Qualifications / Capability Indicators

For indicators of capability for the 511-Cyber Defense Analyst work role, please see Draft NISTR 8193 - National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators.

Section to be populated with updated DoD-8140 Qualification Matrix for 221-Cyber Crime Investigator.

2 APPENDIX: 221-CYBER CRIME INVESTIGATOR TASK ANALYSIS AND KSA MAPPING

2.1 KEY TO READING THE TASK ANALYSIS AND KSA MAPPING

Table 6. Key to Reading the Task Analysis and KSA Mapping

Proficiency	Task Statement	Importance
As Written	Task as written within the NICE Cybersecurity Workforce Framework (NICE Framework).	Overall Importance to Work Role
Entry	*Example behavioral indicator / task permutation for performing this task at an Entry skills proficiency level.*	
Intermediate	*Example behavioral indicator / task permutation for performing this task at an Intermediate skills proficiency level.*	
Advanced	*Example behavioral indicator / task permutation for performing this task at an Advanced skills proficiency level.*	

Table 7. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
ID of K, S, or A	Knowledge, Skill or Ability needed to perform the task as written within the NICE Framework	Competency mapped to the individual K, S, or A.

2.2 221-CYBER CRIME INVESTIGATOR TASK ANALYSIS AND KSA MAPPING

Table 8. T0423 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Analyze computer-generated threats for counterintelligence or criminal activity.	Core
Entry	*Under supervision, analyze computer-generated threats for counterintelligence or criminal activity. Take proper investigative steps.*	
Intermediate	*Analyze computer-generated threats for counterintelligence or criminal activity. Take proper investigative steps.*	
Advanced	*Analyze computer-generated threats for counterintelligence or criminal activity. Take proper investigative steps. Develop techniques/procedures for analyzing/responding to new threats. Provide guidance on complex/novel threats. Communicate situation to decision-makers.*	

Table 9. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0209	Knowledge of covert communication techniques.	Intelligence Analysis
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence
K0070	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).	Vulnerabilities Assessment

Table 10. T0433 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Core
Entry	*Under supervision, conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.*	
Intermediate	*Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.*	
Advanced	*Conduct analysis of log files, evidence, and other information. Develop methods for identifying the perpetrator(s) of a network intrusion or other crimes. Provide guidance on analysis and methods to others.*	

Table 11. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
S0072	Skill in using scientific rules and methods to solve problems.	Data Analysis
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
	branch guidelines, and/or administrative/criminal legal guidelines and procedures.	
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.	Threat Analysis
K0070	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).	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 12. T0103 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Examine recovered data for information of relevance to the issue at hand.	Core
Entry	*Under supervision, examine recovered data for information of relevance to the issue at hand.*	
Intermediate	*Examine recovered data for information of relevance to the issue at hand.*	
Advanced	*Examine recovered data for information of relevance to the issue at hand. Develop new examination methods. Provide guidance for complex data examination.*	

Table 13. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
S0072	Skill in using scientific rules and methods to solve problems.	Data Analysis
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0209	Knowledge of covert communication techniques.	Intelligence Analysis
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.	Threat Analysis
K0070	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).	Vulnerabilities Assessment

Table 14. T0430 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Gather and preserve evidence used on the prosecution of computer crimes.	Core
Entry	*Under supervision, gather and preserve evidence used on the prosecution of computer crimes.*	
Intermediate	*Gather and preserve evidence used on the prosecution of computer crimes.*	
Advanced	*Gather and preserve evidence used on the prosecution of computer crimes. Develop new techniques to gather and preserve evidence. Provide guidance on complex situations.*	

Table 15. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
A0174	Ability to find and navigate the dark web using the TOR network to locate markets and forums.	Web Technology

Table 16. T0112 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Core
Entry	*Under supervision, identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.*	
Intermediate	*Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.*	
Advanced	*Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. Develop new methods for identifying data or intelligence. Provide guidance on how to identify new data or intelligence of evidentiary value.*	

Table 17. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence
K0107	Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.	Threat Analysis

KSA ID	Description	Competency
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.	Threat Analysis
K0070	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).	Vulnerabilities Assessment
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)	Vulnerabilities Assessment

Table 18. T0114 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Identify elements of proof of the crime.	Core
Entry	*Identify elements of proof of the crime.*	
Intermediate	*Identify elements of proof of the crime.*	
Advanced	*Identify elements of proof of the crime. Provide organizational perspective to governing bodies.*	

Table 19. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence

Table 20. T0241 Task Analysis

Proficiency	Task Statement	Importance
As Written within Framework	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Core
Entry	*Use standard equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.*	
Intermediate	*Use specialized equipment and techniques (e.g., JTAG, ISP) to catalog, document, extract, collect, package, and preserve digital evidence.*	
Advanced	*Develop specialized equipment and techniques (e.g., write scripts) to catalog, document, extract, collect, package, and preserve digital evidence. Determine best practices.*	

Table 21. Primary Knowledge, Skills, and Abilities Required to Perform the above Task

KSA ID	Description	Competency
K0118	Knowledge of processes for seizing and preserving digital evidence.	Computer Forensics
K0128	Knowledge of types and collection of persistent data.	Computer Forensics
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	Computer Forensics
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	Computer Forensics
A0175	Ability to examine digital media on multiple operating system platforms.	Computer Forensics
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.	Computer Network Defense
K0110	Knowledge of adversarial tactics, techniques, and procedures.	Computer Network Defense
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, digital scanners, electronic organizers, hard drives, memory cards, modems, network components, networked appliances, networked home control devices, printers, removable storage devices, telephones, copiers, facsimile machines, etc.).	Infrastructure Design
K0209	Knowledge of covert communication techniques.	Intelligence Analysis
K0123	Knowledge of legal governance related to admissibility (e.g. Rules of Evidence).	Legal, Government, and Jurisprudence
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence while maintaining chain of custody.	Legal, Government, and Jurisprudence
K0155	Knowledge of electronic evidence law.	Legal, Government, and Jurisprudence
K0156	Knowledge of legal rules of evidence and court procedure.	Legal, Government, and Jurisprudence

KSA ID	Description	Competency
K0168	Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.	Legal, Government, and Jurisprudence
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	Legal, Government, and Jurisprudence
K0351	Knowledge of applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	Legal, Government, and Jurisprudence
K0070	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).	Vulnerabilities Assessment
A0174	Ability to find and navigate the dark web using the TOR network to locate markets and forums.	Web Technology