STATE OF NEVADA
Department of Administration
Division of Human Resource Management

CLASS SPECIFICATION

TITLE	GRADE	EEO-4	CODE
AG CYBERCRIME INVESTIGATOR II	**40**	**D**	**13.237**
AG CYBERCRIME INVESTIGATOR I	**38**	**D**	**13.238**

SERIES CONCEPT

Cybercrime Investigators in the Attorney General's Investigations Division perform criminal investigations and analysis involving a variety of highly specialized forensic examinations performed on electronic devices or networks that can be programmed or can store or convey information in any form that is used in suspected criminal violations of State and/or federal laws pertaining to a specific program or regulatory area which includes, but is not limited to, Medicaid fraud, workers' compensation fraud, consumer protection, public integrity, human trafficking, missing children, financial fraud, alleged criminal offenses committed by State officers or employees, Internet Crimes Against Children, terrorism, drug crimes, identity theft, crimes against persons or property, and all types of conflict of interest cases submitted by outside agencies.

Provide technical expertise and assistance to State, federal, and local law enforcement in computer forensics related matters; obtain and maintain investigative computer forensics field equipment; obtain and maintain computer forensics laboratory equipment including updating hardware and software licenses.

Perform specialized investigations and computer forensic examinations of complex cases that may involve multiple criminal violations, suspects and jurisdictions and may be sensitive in nature.

Conduct interviews of witnesses, victims, and suspects; conduct forensic examinations of computers and other electronic devices and corresponding electronic data storage media to obtain information regarding the alleged criminal activity in an effort to complete investigative assignments in consideration of agency priorities, goals and objectives; review information received to determine possible criminal activity, validity of information and appropriate jurisdiction.

Conduct field surveillance and background investigations; participate in undercover "sting" operations in order to establish leads, solidify evidence, and develop probable cause; use electronic audio/video recording equipment or personally conduct transactions with suspects to gather evidence, develop leads and establish probable cause; establish proof of facts and evidence; and review case findings with appropriate parties.

Conduct research; gather and preserve evidence; take photographs and video; and transport, secure, prepare and analyze evidence by following proper evidentiary procedure.

Search law enforcement databases to include, but not limited to, National Crime Information Center (NCIC), National Criminal Justice Information System (NCJIS), Shared Computer Operations Protection Enforcement (SCOPE), Tiburon and the Department of Motor Vehicles.

Prepare reports on computer forensic examination results and prepare evidence for presentation; testify as an investigator and as a computer forensics expert in court or other proceedings as required.

Prepare investigative reports encompassing all significant events and facts pertaining to the case elements, outline and summarize violations committed, and submit and/or present findings to the prosecutor; develop illustrative charts/slides to explain analytical forensic findings to a lay audience; prepare, obtain and execute legal documents such as affidavits, search warrants, arrest warrants, and subpoenas to continue the criminal justice process and criminal prosecution.

SERIES CONCEPT (cont'd)

Develop case files and maintain case logs and reports; document investigative activities in order to develop and formulate facts and leads, establish patterns and trends, determine motives, and support enforcement actions.

Maintain various reports such as daily activity reports, case summaries, arrest reports, and vehicle reports; utilize information to develop and report statistical data and to substantiate program budget expenditures.

Continually update and develop skills regarding new computer technology, hardware and software tools, and attend training to maintain and acquire knowledge of trends and developments in the field of computer forensics.

Conduct training programs and outreach regarding agency services, specialized functions and/or programs to other law enforcement agencies, State and local government officials, and the general public or community groups to develop understanding and awareness related to the use and abuse of digital information and devices.

Perform related duties as assigned.

****

DISTINGUISHING CHARACTERISTICS

Enforcement powers are that of peace officers and incumbents have police powers for the enforcement of the provisions of the Nevada Revised Statutes and federal laws relating to any reported or observed criminal activity. AG Cybercrime Investigators carry firearms in the performance of their duties. All positions in this class series are, at a minimum, P.O.S.T. Category II certified, upon permanent status.

In addition, AG Cybercrime Investigators perform specialized casework assignments on a statewide basis which involve the identification, seizure and examination of digital devices used in furtherance of criminal acts.

****

CLASS CONCEPTS

AG Cybercrime Investigator II: Under general direction, incumbents are expected to perform the full range of duties as described in the series concept; however, the primary responsibility is investigating complex cases and conducting computer forensic examinations related to the use of computers and other technological devices by perpetrators in an effort to assist, conceal or carry out acts in violation of State and/or federal laws. Positions allocated to this class provide computer forensic services to other criminal investigators not trained in computer forensics. They also independently conduct investigations and computer forensic examinations related to the most difficult assignments involving cases of a high profile or sensitive nature, or multiple program or criminal violations. Duties are distinguished from the AG Cybercrime Investigator I class by greater complexity and independence in performing job assignments. This is the advanced journey level in the series.

AG Cybercrime Investigator I: Under limited supervision, incumbents perform the full range of duties as described in the series concept. Incumbents conduct investigative assignments and computer forensic examinations related to the use of computers and other technological devices by perpetrators in an effort to assist, conceal or carry out acts in violation of State and/or federal laws.

Positions allocated to this class provide computer forensics services to other criminal investigators not trained in computer forensics. Work is closely reviewed for accuracy. This is the journey level in the series.

****

MINIMUM QUALIFICATIONS

SPECIAL REQUIREMENTS:

- Persons offered employment in this series must submit to a background, medical, and psychological evaluation.
- A valid driver's license is required at the time of appointment and as a condition of continuing employment.
- AG Cybercrime Investigator I must obtain Certification by the International Association of Computer Investigative Specialists (IACIS) or Basic Computer Evidence Recovery Training (BCERT) at the National Computer Forensics Institute within 18 months of employment and as a condition of continuing employment.
- AG Cybercrime Investigator II must have current Certification by the International Association of Computer Investigative Specialists (IACIS) or Basic Computer Evidence Recovery Training (BCERT) at the National Computer Forensics Institute at the time of appointment and as a condition of continuing employment.

INFORMATIONAL NOTES:

- Applicants must meet the minimum standards for appointment as a peace officer as established in the Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC).
- AG Cybercrime Investigator I must obtain and maintain, at a minimum, Nevada POST Category II certification within one year of appointment and as a condition of continuing employment.
- AG Cybercrime Investigator II must maintain, at a minimum, Nevada POST Category II certification as a condition of continuing employment.
- A bi-annual qualifying score of 80 or better with a firearm will be required.
- Incumbents may be required to obtain and maintain a Top Secret National Security Clearance issued by the FBI.

AG CYBERCRIME INVESTIGATOR II

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in computer science, information technology, computer forensics, criminal justice, police science, or closely related field; current, at a minimum, Category II POST certification in Nevada; and three years of criminal investigation and law enforcement experience involving standard investigative and enforcement techniques utilized to enforce local, State and/or federal and agency laws and regulations, preparation of detailed investigative reports, implementation of agency program goals and objectives, handling of digital evidence, and experience performing forensic examinations of computers, networks or other digital devices for a law enforcement agency; **OR** graduation from high school or equivalent education; current, at a minimum, Category II POST certification in Nevada; and five years of experience as described above; **OR** two years of experience as an AG Cybercrime Investigator I in Nevada State Service; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application):
Working knowledge of: the use of automated forensic tools to identify, collect, preserve, and extract digital evidence from a variety of computers, platforms, operating systems, mobile devices, e-mail and messaging systems; criminal laboratory protocols related to packaging, submission, preservation, and storage of digital and computer evidence; computer forensic examination procedures, and electronic search methods used to analyze, identify, extract, and preserve digital and computer evidence; and the reporting of examinations including search techniques, recovery of deleted files and digital evidence identified in support of criminal allegations. **Ability to:** collect, organize, verify, and analyze investigative data; interpret and apply local, State, and/or federal laws, codes, regulations, and agency policies; conduct searches, seizures and arrests; conduct forensic examinations of a variety of digital devices including computers, mobile devices and other storage media; communicate clearly and concisely verbally and in writing; skillfully present courtroom testimony that involves both technical and non-technical subject matter; *and all knowledge, skills and abilities required at the lower level.*

MINIMUM QUALIFICATIONS (cont'd)

AG CYBERCRIME INVESTIGATOR II (cont'd)

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job):
Detailed knowledge of: applicable local, State and/or federal laws, codes, statutes, regulations, and agency policies governing investigation functions appropriate to the area of assignment. **Working knowledge of:** the design, implementation, administration and securing of networks; the acquisition of mail servers, database servers and large data stores; mainframe basics and acquisition techniques; intrusion detection techniques used to discover and determine the existence or presence of evidence related to any wrongful act of entering, seizing, or taking possession of the property of another. **Ability to:** plan, coordinate, and expedite computer forensics investigations; conduct the most complex technical forensic examinations of a variety of digital devices, including networks or unconventional storage media; coordinate, set priorities, assign, and review computer forensic work of other professional staff when necessary; evaluate the needs for training and equipment in the area of assignment; *and all knowledge, skills and abilities required at the lower level.*

AG CYBERCRIME INVESTIGATOR I

EDUCATION AND EXPERIENCE: Bachelor's degree from an accredited college or university in computer science, information technology, computer forensics, criminal justice, police science, or closely related field; current, at a minimum, Category II POST certification in Nevada within one year of appointment and as a condition of continuing employment; and one year of criminal investigation and law enforcement experience involving standard investigative and enforcement techniques utilized to enforce local, State and/or federal and agency laws, preparation of detailed investigative reports, implementation of agency goals and objectives, and handling of digital evidence; **OR** graduation from high school or equivalent education; current, at a minimum, Category II POST certification in Nevada; and three years of experience as described above; **OR** one year of experience as an AG Criminal Investigator I or Criminal Investigator I in Nevada State service; **OR** an equivalent combination of education and experience as described above. *(See Special Requirements and Informational Notes)*

ENTRY LEVEL KNOWLEDGE, SKILLS AND ABILITIES (required at time of application):
Working knowledge of: applicable local, State and/or federal laws, codes, statutes, regulations, and agency policies governing investigation functions appropriate to the area of assignment; court procedures and documents; legal rights and rules of evidence; civil, criminal or administrative proceedings; chain of custody of evidence; laws of arrest, search and seizure; interview and interrogation techniques; criminal investigative techniques and enforcement procedures; standard computer operating systems, software and applications; a broad spectrum of computer hardware, networks, mobile computing devices, media platforms and storage devices; use of digital evidence in criminal investigations; and basic computer forensic tools and techniques used to acquire digital evidence. **Ability to:** read, understand and apply State and/or federal laws, codes, statutes, regulations, and agency policies; collect evidence; communicate effectively with a wide variety of public contacts; prepare detailed written reports; provide court testimony; identify types of digital evidence used in support of criminal allegations; and perform public speaking activities.

.

FULL PERFORMANCE KNOWLEDGE, SKILLS AND ABILITIES (typically acquired on the job):
(These are identical to the Entry Level Knowledge, Skills and Abilities required for AG Cybercrime Investigator II.)

This class specification is used for classification, recruitment and examination purposes. It is not to be considered a substitute for work performance standards for positions assigned to this class.

	13.237	13.238
ESTABLISHED:	12/19/17UC	12/19/17UC