Information Security Officer Information Guide

What to Expect on the Structured Interview

June 2020

Jefferson County Commission

Human Resources Department

Employee Selection Division

Table of Contents

***************Coronavirus (COVID-19) Information***************

Please note, due to recent events concerning the coronavirus pandemic (COVID-19), CDC guidelines will be followed for all secondary selection procedures administered by the Employee Selection Division of the Human Resources Department. Additional precautionary measures that may be taken include:

1. **Disinfecting common areas of the testing facility - pre-interview and post-interview.**
2. **Restricting the number of candidates and/or exams we administer to limit the total number of individuals in the testing facility.**
3. **Limiting the number of on-site Human Resource test administrators or staff members.**

I. INTRODUCTION

The purpose of this information guide is to help explain what to expect on the upcoming structured interview (or "test") for the Jefferson County Information Security Officer position. It will also give you information on how to prepare for the test. This booklet contains information about the interview process, including:

- Introduction
- Interview Description and an Example Question
- Content Measured by the Structured Interview
- Preparing for the Interview
- Additional Information for Taking the Interview
- Contact Information

You were determined to be minimally qualified for this job by the Personnel Board of Jefferson County, and your name was placed on a list and shared with us here in the Human Resources Department of Jefferson County Commission. This step in the process was considered the primary selection process.

Now you will be participating in the secondary selection process which is a recorded structured interview. You must take the structured interview in order to be considered for this position. Please remember that the material in this booklet is designed to help prepare you for the test. You will not need the material in this booklet at the time you actually take the test. **Therefore, you will not be allowed to carry this booklet into the interview session.**

II. TEST DESCRIPTION

The upcoming test for Information Security Officer consists of a structured interview. There will be approximately 9 scenarios and associated focusing questions on the interview. The scenarios will be about issues, situations, responsibilities, activities, incidents, etc., which a new Information Security Officer may have to address. You will have time beforehand to prepare your response to some or all parts of the interview. After the preparation period is over, you will begin your interview session. The scenarios and focusing questions will be narrated. You will respond orally to each scenario and all focusing questions. Your response will be recorded. You will have a specified number of minutes to respond to each question. If you complete your response before the allotted time has elapsed you must wait until the time expires and a new scenario is presented.

On the day of the test, you will be provided with a test preparation guide that contains some or all of the actual scenarios and focusing questions you will respond to during the interview. You will have a specified number of minutes to read through the scenario and focusing questions and prepare your responses. The preparation period includes any time you spend reading the interview instructions.

While you are reviewing the scenarios and associated focusing questions, you may make notes for your use during the interview. **Raters will only be evaluating you on what you say during the actual interview session**. They will not evaluate what you have written down in your notes. Only your verbal responses will be scored.

When it is time for your interview to start, you will be prompted by the computer monitor screen in your testing room. You will be the only candidate in the testing room. When the interview starts, you will see information on screen and hear the same information read by a narrator.

The narrator will present each scenario, or question, verbally. After each scenario, the narrator will present a set of focusing questions. The focusing questions will also be presented in writing either on a sheet of paper or on a video monitor. To complete the test, you must verbally respond to each scenario

and its associated focusing questions. You may use your notes when providing your response; however, your notes will not be evaluated. Only your verbal response will be assessed.

After each scenario and its associated focusing questions have been presented, you will hear the instruction, "your response period begins now." The time remaining to answer the question will be shown on a video monitor or on a timer. You will then have a specified number of minutes to respond to each scenario and associated focusing questions. At the end of each pre-specified time period, you will hear the command "STOP! Your time is up." Evaluators will ignore any information you provide after the command to stop has been issued. You will not be able to use time from a subsequent scenario to complete a response to an earlier scenario.

Your responses will be recorded. It is important that any audio or video equipment remain in place; therefore, do not touch any of the equipment at any time. You could be disqualified from the interview process for tampering with any of the equipment. If there is a problem with the equipment, please raise your hand and keep it raised until a test monitor enters your room. You are responsible for making sure you speak loudly and clearly enough to be understood by the evaluators reviewing your recording. A normal conversational tone as used in a meeting setting is sufficient.

Remember, there will be approximately 9 scenarios and associated focusing questions. Each scenario and focusing question will be read aloud prior to your response time beginning. In your response, be sure to answer all of the focusing questions presented. Keep in mind the following things when responding:

- More detail is better than less detail. That is, more details which show one's knowledge, skills and abilities relevant to the question may improve a candidate's evaluation
- The evaluators will not "read in" to what you say
- Your responses will be evaluated against a defined set of performance standards
- You should answer all focusing questions related to each scenario
- Be sure to talk about what you would do and why

Sample Question

The following question is presented as an example of the form or type of scenarios with which you will be presented. Please note that the content, or subject matter, of the actual interview scenarios will vary and may or may not be similar to that of the questions presented below. The scenarios to which you will respond during the interview will be related to the job for which you are applying.

Example

The department that you work in recently purchased some new equipment. Today, you are able to use the new equipment for the first time. You have been told that the new equipment is similar to what you have had previously. While you are using the new equipment, it stops working and shows an error message that you have never seen before.

Focusing Question(s)

What are the next steps that you would take to determine the meaning of the error message and continue with your work?

III. CONTENT MEASURED BY THE TEST

An analysis of the Information Security Officer job was conducted prior to developing the structured interview. Employees who work in this position, and their supervisors, participated in this process.

When the job analysis study was completed, the results showed that a new employee in the Information Security Officer position may perform several of the duties listed below, including:

- Responds to network and system attacks by establishing an incident response plan, identifying key assets, and creating and developing a network and systems security team.
- Procures and/or manages inventory (i.e., supplies and equipment) to ensure the products and services are available to meet the operational needs of each department.
- Conducts information security risk assessments (including disaster recovery and contingency planning and implementation), responds to and reports/documents security breaches or information security threats, and takes corrective action to prevent future occurrences in order to comply with scheduled audits.
- Ensures maintenance and upgrade of networks, systems, and equipment in order to ensure effective, appropriate, and secure functioning of all organizational information systems and technology.
- Produces reports, letters, and other types of written correspondence designed to document activities and efforts, share and communicate information, and provide instruction and/or guidance on organizational and departmental practices.
- Engages in activities designed to ensure professional development, awareness of developments in the field, and knowledge of relevant practices, rules, laws, policies, and/or guidelines.
- Developments and executes strategic planning and vision related to information security and services by collaborating with department heads and upper management to establish information security goals and objectives.
- Supervises staff by assigning and distributing work, directing staff in their job duties, monitoring progress of work, providing feedback and/or training.

The study of the job also showed that a number of knowledge, skills, and abilities were very important and needed from the moment a person becomes a (that is, before receiving any training for the Information Security Officer job.). These knowledge, skills, and abilities include:

- Knowledge of client server and network based applications protocols.
- Knowledge of computer operating systems such as UNIX and WINDOWS.
- Knowledge of formal procedures for project management and reporting tools.
- Knowledge of high-performance computer systems used for large-scale computing purposes and requiring greater availability and security than a smaller-scale machine.
- Knowledge of networking capabilities and methods (e.g., TCP/IP, Vmware, VPN).
- Knowledge of the principles and practices of risk management.
- Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- Knowledge of data backup and restoration concepts.
- Knowledge of penetration testing principles, tools, and techniques.
- Knowledge of system administration, network, and operating system hardening techniques.
- Skill in assessing the robustness of security systems and designs.
- Skill in conducting application vulnerability assessments.
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
- Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
- Skill in developing insights about the context of an organization's threat environment.
- Skill in performing impact/risk assessments.

- Skill in reviewing logs to identify evidence of past intrusions.
- Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
- Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).
- Skill in using a Linux Operating system.
- Skill in verbally delivering information in a clear and concise manner to an audience.
- Skill in understanding and applying concepts of statistics and probability theory in order to identify trends, problems, and relationships among data.
- Skill in conducting oneself in a calm and professional manner in stressful situations.
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
- Ability to adjust to changing work demands, procedures, technology, and/or priorities.
- Ability to learn unfamiliar material/information quickly and accurately.
- Ability to anticipate the needs and interests of customers and clients.
- Ability to assess the performance of other individuals to ensure work is performed appropriately and/or take corrective action.
- Ability to assign and monitor the work of subordinates.
- Ability to commit, entrust, or transfer tasks or responsibilities to another.
- Ability to guide and direct the accomplishment of work through subordinate staff.
- Ability to influence, motivate, and inspire employees.
- Ability to motivate and encourage others to a course of action or goal.
- Ability to review work and evaluate it against established standards, procedures, laws, or codes to determine any discrepancies between how the work was performed and how it should be performed.
- Ability to listen to and understand information and ideas presented through spoken words and sentences.
- Ability to orally communicate information and ideas so others will understand.
- Ability to analyze a problem from different perspectives and generate potential solutions that are practical and effective.
- Ability to analyze information and draw valid conclusions.
- Ability to combine information in order to form logical conclusions or to identify relationships between different pieces of information.
- Ability to use logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions, or approaches to problems.
- Ability to demonstrate honest behavior in all work tasks and responsibilities.
- Ability to work in an environment that requires strict adherence to instructions, standards, and/or procedures.
- Ability to determine how a system should work and how changes in conditions, operations, and the environment will affect outcomes.
- Ability to manage your time in order to accomplish objectives within given timeframes.
- Ability to stay abreast of developments in the field/industry.
- Ability to work productively and effectively under conditions of high stress, such as tight deadlines, heavy workloads, or emergency situations.
- Ability to work without close supervision or significant amounts of direction/guidance.
- Ability to read and understand information presented in diagrams, blueprints, maps, specifications, or other pictorial displays.

- Ability to communicate information and ideas in writing to a variety of audiences in a clear, concise, and organized manner, free from spelling, grammar, and punctuation errors.
- Ability to read and understand information and ideas presented in writing.

The structured interview will give you an opportunity to demonstrate many of the knowledge areas, skills, and abilities you have just read.

As discussed, the upcoming test for Information Security Officer is a structured interview involving reading and listening to questions, taking notes to prepare, and providing verbal responses. If you require special testing accommodation to participate in this test, you should notify Jefferson County Human Resources immediately using the contact information at the end of this guide.

In the remainder of this "What to Expect" Booklet, you will read about ways to prepare to take the test, what to bring to the test, and whom to contact if you have a question.

IV. PREPARING FOR THE TEST

A. General information on "What to do before the test":

Here are some suggestions for what to do before the test. This includes getting to the testing place on time and with the proper things that you will need to take the test.

1) Be well rested. Get a good night's sleep for several nights in a row before the interview.
2) Allow plenty of time to get to the test. If you are rushed and late, you will be upset when you get there. Plan to arrive at least 15-20 minutes before earlier than the scheduled time for check-in. Due to the nature of the test and the number of candidates that must be processed, NO exceptions will be made to accommodate individuals arriving more than 15 minutes after their scheduled check-in time.
3) Come in to the test dressed comfortably. You will be there for up to two hours.
4) Do NOT bring any electronic communication devices (e.g., cell phones, laptops, tablets, smart watches, etc.) with you to the interview. If you bring a cell phone or any other electronic communication device, you will be asked to return it to your car. Jefferson County will not confiscate them or "hold" them for you during the interview. You must comply with this rule in order to be admitted and you will still be subject to the check-in deadline. Using any communication device after you have checked into the test site will be considered a violation of test security and you will be disqualified. ALL electronic communication devices are prohibited from the testing facility (e.g., cell phones, tablets, smart watches, cameras, etc.).
   a) If any device is seen, heard, or used during the interview process it will be considered a violation of test security and you will be disqualified and dismissed from the interview process.
   b) You are allowed to bring reading materials, such as magazines or books not related to the position or interview.
5) Do not bring any of your study or reference materials to the test. This includes any notes, manuals, source documents, reference materials, or study materials that you have used or created to prepare for the test.
6) Do not bring this booklet to the test location. You will not be permitted to bring it in. All the materials you need for the test will be given to you at the test.
7) You should read this booklet to get comfortable with the test process.
8) You should read this booklet to understand which job duties, knowledge, and abilities are important for the Information Security Officer job.
9) You should bring the confirmation email that you have received from Jefferson County to the testing location. The confirmation email lists the name of the test (i.e., Information Security Officer), the place you should go to in order to take the test, and the time, day, and date of the test.

10) You must bring valid PHOTO IDENTIFICATION (i.e., Valid Driver's License, Valid Nondriver ID, Valid Photo Voter ID Card, Valid State Issued ID [Alabama or any other state], Valid Federal issued ID, Valid US passport, Valid Employee ID from Federal Government, State, County, Municipality, Board or other entity of the state, Valid student or employee ID issued by a state or private institution of higher learning [including postgraduate technical or professional schools], Valid Military ID, or Valid Tribal ID). You will not be allowed to enter the test location nor take the test without your photo identification.

B. General information on "What to do during the test":

1) Some people are nervous when they take tests. Up to a point, there is nothing wrong with that. Whenever you are going to do something important, it is good to feel a bit nervous. It is nature's way of getting you warmed up and ready, like an actress or actor about to go out on stage for a performance.
2) However, it is not good to be so nervous that all you can think about is how nervous you are. You need to keep your mind on the test questions, and not on your feelings. To improve your ability to do that, you will find useful ideas in this booklet on how to prepare for the test and what to expect. **The more prepared you are, the more comfortable and less nervous you will feel during the test.**
3) Several things that you can do that will make you feel more comfortable taking the structured interview including: following the guidelines presented in this booklet on what to expect on the test and how to prepare for the test; becoming familiar with what the structured interview process will be like (including reading the sample question); and, understanding the test instructions.
4) You must not leave the room in which you are taking the interview unless you are told that you may do so. Once the test begins, you must remain in your room. There will be Test Monitors nearby at all times. They will be available to assist you if you have any problems.
5) You will be given the opportunity to use the restroom, stand, and stretch throughout the time you are at the testing location. You should use these opportunities as necessary. Once the test begins, you will not be able to stop the process to use the rest room.
6) You are not to open any test material or instructions or begin working on the test until you are instructed to do so.
7) During the preparation and testing period, you are not to use any materials other than what has been provided during the testing session.
8) Candidates making any disturbances or caught cheating will be disqualified from the test.
9) Test Monitors will not interpret test questions for you. However, they can assist you with any problems, such as mechanical difficulties or equipment breakdowns.
10) There will be an audio recorder in the room in which you take the test. The audio recorder will be used to record your spoken responses to the test.
11) You should speak in a normal speaking voice when you are required to give spoken responses to questions. It is not necessary to shout, but do not talk in a whisper either. Simply speak in a normal voice.
12) On the day of the test, you will be provided with a test preparation guide to help you prepare to respond to the structured interview questions.

V. ADDITIONAL INFORMATION FOR TAKING THIS TEST

The following information will help you prepare to take the structured interview.

A. What To Bring To the Test

Please remember to bring to the test the confirmation email that you received from Jefferson County.

You must bring a PHOTO IDENTIFICATION to the test location. This might be a valid driver's license, a military identification card, a passport, etc. You only need to have one form of photo identification. You will **not be allowed** to enter the test location or take the test without your photo identification.

You should plan on bringing your own beverages and food to snack on during the day. You will be onsite for up to two hours. Once on the test site, you will NOT be permitted to leave to get food or drinks. You should also bring something to read such as a book or magazine. The reading material should be for pleasure only. You **may not** bring outside test-related materials into the test. All written materials needed for taking the test will be provided. You do not need to bring writing utensils with you to the test—they will be provided to you.

B. What Not To Bring To the Test

Do **NOT** bring this Booklet to the test location. You will not be permitted to bring it in the testing room.

Do **NOT** bring any of your study materials to the test. This includes notes, manuals, and other study materials.

Do **NOT** bring any electronic communication devices (e.g., cell phones, laptops, tablets, smart watches, cameras, etc.) with you to the interview.

C. Effective Note Taking

The structured interview asks about issues, situations, responsibilities, activities, incidents, etc. which a newly hired Information Security Officer may have to address. On the day of the test, you will be given a chance to look over the questions that you will be asked on the test before you start the interview. You will have a chance to think about your answers for the test, and you should take notes to help guide your responses. Good notes contain the essential or important details. The notes do not need to be written in complete sentences. You are the only one who needs to be able to read and understand your notes. Your notes will not be graded. Your notes will be collected at the end of the interview.

Why Take Notes?

There are several good reasons to take notes during the preparation phase of the test process.

- In order to take notes, you are forced to carefully consider the information being given.
- Taking notes can help you remember. Notes you take in your own words are easier to understand and remember.
- Writing down notes may actually make the information clearer to you.
- The notes will help you respond to the interview scenarios and focusing questions.
- Having notes can help you feel less anxious or nervous while taking the test.

VI. TEST CONTACT INFORMATION

General Questions about the Test

If you have questions about the test administration, you may contact the Employee Selection Division at (205) 214-5518 or careers@jccal.org. Jefferson County employees are not allowed to divulge, and do not have access to, specific information about the content of the test.

Reasonable Accommodation

If you would like to request special testing accommodations or have any questions concerning the test site or testing conditions, please contact Sarah Freed at 205-583-8321 or freeds@jccal.org.