TEST SECURITY STANDARDS FOR ONLINE PROCTORING

CAVEON TEST SECURITY

INTRODUCTION

The purpose of the Test Security Standards for Online Proctoring is to provide a set of objective and practical standards for securely administering tests using online proctors. While there are many additional practical and procedural concerns regarding online proctoring, Caveon's standards focus solely on those related to test security.[1]

Due to the global pandemic of 2020 and the resulting near-universal reliance on online proctoring for every type of important exam, it has become clear that standards relating to the security considerations of remote proctoring are necessary. While it is true that with a few minor changes, much of the content within these standards could apply to on-site proctoring as well as online proctoring, the current global climate has resulted in widespread confusion, concern, and anxiety regarding how to safely adopt online proctoring. Caveon seeks to alleviate some of this anxiety by sharing these standards.

Online Proctoring

On-site proctoring occurs in a room with test takers. The proctor is physically present and is responsible for both the administrative and security-related tasks. In comparison, with online proctoring, the proctor is not physically present but can view, listen, and interact with the test taker. This is done using computers, the internet, webcams, and other technology (examples of available technology can be viewed in this article).[2]

Like on-site proctors, online proctors are responsible for both administrative and security tasks. Administrative tasks include responsibilities such as test administration intake, customer service, and technical support that are unrelated to test security (these proctor duties are outlined in this white paper). With regards to security, an online proctor's responsibilities include:

[1] By focusing these standards on test security, Caveon does not mean to suggest that other concerns related to the administration of tests using online proctors are not important. Indeed, there are well-founded concerns about equity, accessibility, privacy, and fairness that must be addressed when it comes to the administration of tests using online proctors. However, those important issues are not within the scope of the standards listed here.

[2] Test administration intake does not include the authentication or identification of the test taker. It simply refers to the operational tasks of welcoming the test taker, providing general non-security instructions, etc. Authentication and identification are covered below as part of the test security features we recommend in online proctoring systems.

1. Authenticating the test taker (making sure an examinee is authorized to take the test)
2. Ensuring the test taker is connected to the internet and correctly using the appropriate technology, helping the proctor detect and control security threats (e.g., programs that capture responses or keep test takers from accessing forbidden web resources)
3. Monitoring the exam administration for security violations and following up with the appropriate actions if a violation is discovered (e.g., the proctor could offer warnings, pause the test, terminate an exam session, etc.)

These proctor security responsibilities are the focus of these standards.

Threats and Test Security Solutions

Caveon has produced a list of threats covering both the theft of test content and cheating. Most of these threats occur during test administration, and some of them can be detected by an alert proctor. A firm grasp on these threats and the risks they pose is necessary to understand the standards being proposed in this document. Understanding these threats is the starting place for all effective test security efforts. When determining which security solutions to implement (including proctoring), a testing program and/or services provider should prioritize solutions that address the threats that pose the highest risks to the program.

The goal of test security, first and foremost, is to protect the valid use of test scores. This includes (if possible) preventing or inhibiting all forms of cheating and test theft. Protecting the valid usefulness of test scores involves three separate forms of defense:

1. **Prevention**
   Measures that make it difficult or impossible to steal content or to cheat.
2. **Detection/Reaction**
   Measures that detect threats before or during a security breach, and that automatically trigger a prepared plan for dealing with whatever threat or breach has been detected.
3. **Deterrence**
   Measures that convince those who would cheat or steal content that the effort isn't worth it.

[3] Cheating is defined as any attempt, successful or not, to increase a test score inappropriately. Test theft is defined simply as efforts to illegally steal test content. Learn more in this white paper.

While online proctoring can contribute to the overall effectiveness of the test security plan for a given program, proctoring is not a comprehensive test security solution on its own (learn more about the effectiveness of proctoring and its relation to prevention, detection, and deterrence in this article). Any security plan that includes the use of online proctoring should maximize its effectiveness by combining all three of those solutions—prevention, detection/reaction, and deterrence.

For example, a test that is being proctored online might use AI-assistive proctoring technology (detection) while convincing test takers about the success of the proctoring methodology (deterrence). The test might also be designed with items that prevent theft (prevention), meaning the online proctors can ignore the many indications of threats that focus on stealing test content. In all, the use of several solutions within each category of prevention, detection/reaction, and deterrence is recommended.

CAVEON STANDARDS FOR ONLINE PROCTORING

These standards have been written to maximize online proctoring's impact on the three categories of solutions above: Prevention, Detection/Reaction, and Deterrence.

1 Authentication and Identification

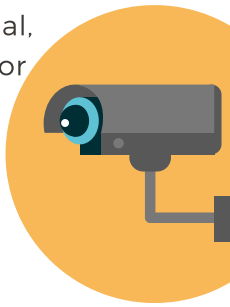
Online proctoring systems must confirm that a prospective test taker is authorized to sit for the exam.

1.1 The online proctors themselves should NOT participate in the authentication or identification processes that confirm a test taker's right to sit for the exam.

Explanation: Identification documents can be easily fabricated. These are difficult if not impossible to detect (even by on-site proctors). The problem is made worse by having to validate ID documents through a webcam.

1.2 Online proctoring systems should use one or more automated biometrics to authenticate (not necessarily identify) test takers. Biometrics solutions that avoid privacy concerns should be chosen.

Explanation: Some types of biometrics (facial recognition, fingerprint, etc.) lead to obvious privacy concerns. Others (such as using keystroke patterns entered to arbitrary phrases) avoid the privacy concerns by being unconnected to obvious identification systems. The authentication is only intended to verify that the prospective test taker currently waiting to take an exam is the person who signed up and provided similar personal biometrics when registering for the educational, certification, or licensure program. More than one biometric can be combined for greater verification accuracy if desired.



2 Observation

Online proctoring provides for the effective visual and auditory observation of the test taker and the test environment throughout the exam session.

2.1 Test takers should be warned or required in advance to remove private information from the testing area, or to sit for the test in a quieter, more neutral home or work location.

Explanation: Because the online proctor is able to observe (both see and hear) the testing environment, it is possible that a test taker's private information could be revealed. The online proctoring system needs to do its part to protect the rights and private information of test takers.

2.2 With good assistive technologies, online proctors should be able to monitor more than a single test taker at a time.

Explanation: The optimal ratio of test takers to online proctors for a testing program or its vendor will depend on many factors. Among these factors included are the number and quality of additional test security assistive technologies that are employed during the exam. For example, there are secure test and item designs available today that eliminate the need for online proctors to detect most forms of cheating and test theft. This means that the test is more secure while limiting the demands on the proctor. As such, the ratio can be increased significantly.

Also, if the online proctoring system includes technology to automatically detect excessive other infractions (e.g., noise, talking, or movement) and then alerts the proctor, this further reduces the need for stringent and vigilant observation, allowing the ratio to be increased even further.

Finally, the ratio is affected by how much cheating and theft goes undetected, a number that can be determined in an ongoing way using metrics from data forensics or web monitoring efforts

2.3 The online proctoring system includes the visual observation of the workstation, desk surface, and keyboard.

Explanation: The more a proctor or the proctoring system is able to see of the area around the workstation, the more likely they will be able to detect the use of cheat sheets, cell phones, and other prohibited items. Being able to only view a test taker's face and shoulders through a laptop camera during the exam poses a serious security risk that is actually introduced by a limited proctoring system.

2.4 The online proctoring system includes the relatively unobstructed and clear observation of the environment in which the test is being administered.

Explanation: The more a proctor or the proctoring system is able to see of the testing environment, the more likely they will be able to detect the use of notes posted on walls, other monitors being used, etc. Being able to only view a test taker's face and shoulders through a laptop camera during the exam poses a serious security risk that is actually introduced by a limited proctoring system.

2.5 The online proctoring system includes the monitoring of sound, such as noises, music, and voices, in the testing environment.

Explanation: The more a proctor or the proctoring system is able to hear from the testing environment during the testing session, the more likely they will be able to detect the use of cell phones, oral collaboration with others, unexpected distractions, and even irrelevant discussions with others.

3 Device Control and Monitoring

The test administration device (laptop, desktop, phone, or tablet) is sufficiently secured and monitored throughout the testing session.

3.1 With traditionally designed exams (fixed forms, static multiple-choice items, etc.), it is necessary to restrict the test taker from unauthorized access to the internet and other general (e.g., hard drive) or specific (e.g., a particular program) computer-based resources.

Explanation: Technology that can restrict testing devices and limit access to external resources should be used for most exam types. By simply monitoring test taker activities on the device, it is possible and relatively easy to detect inappropriate or excessive activity, which can be dealt with quickly by the online proctor. Keep in mind that some test or item designs (e.g., computerized adaptive tests, linear on-the-fly tests, tests made up of unique forms, etc.) may not require the use of a restrictive programs if those designs display items of sufficient and random variability, making some forms of cheating irrelevant.

3.2 Device input and output activity must be monitored and recorded at all times. Inappropriate activity should trigger an alert to an online proctor.

Explanation: Inappropriate or excessive input and output activity may indicate attempts to exit the testing system, to communicate with others, to access inappropriate resources, etc.

4 Interaction/Control

The online proctoring system provides the capability for interaction with the test taker and the testing system both before and throughout the test administration session.

4.1 The online proctor can communicate with and collect information from the test taker prior to and during the testing session.

Explanation: A communication system (such as an immediate chat session) is necessary if the online proctor observes a security rule being broken and must learn more directly from the test taker. Likewise, the test taker may need to ask a special request of the proctor, such as taking an emergency break.

4.2 The online proctor can control the testing session through pausing, un-pausing, suspending, or canceling the test.

Explanation: Online proctoring systems must allow a proctor to pause the test, particularly when instituting a chat session or if the test taker loses connectivity to the proctor. It is contrary to professional testing standards to interrupt and talk with a test taker without pausing the test timing. It may also be necessary at times to un-pause, suspend, or cancel the test.

4.3 The online proctoring system provides a way for examinees to seek help regarding test security rules and measures prior to the start of testing and during the testing session.

Explanation: A test taker may be unclear regarding security rules and may wish to ask the online proctor. The ability to initiate a chat session should be available to the test taker. Depending on the nature of the question, the proctor may choose to pause the timing of the test during the interaction.

4.4 The online proctoring system provides a way for examinees to provide feedback regarding the test security effectiveness of the online proctor or the online proctoring system.

Explanation: The online proctoring system should provide a way for test takers to give opinions or describe experiences about the online proctor or the online testing system, particularly about test security features and activities. This option should be made available after the test session has ended.

5 Recording Logs

The online proctoring system provides for the video and audio recording of the testing session, including interactions between the test taker and the online proctor.

5.1 The video and audio relevant to a security incident is recorded and stored, including interactions between the test taker and online proctor, system logs, proctor logs, decisions made, etc.

Explanation: It may be necessary to understand or defend the actions of an online proctor (or the online proctoring system) during a test administration event, whether to a security committee or in a legal proceeding. Faithful recordings of all security-related activities are critical records that protect the rights of all parties involved.

5.2 Test security-related information should be stored for as long as is deemed necessary.

Explanation: The process to investigate test security incidents, as well as the process for appeals, may take months or years. At least for test security purposes, when it is determined that testing data are not needed, the data should be deleted as soon as possible.

5.3 Test security stored information should be easily accessed, and that access should be managed.

Explanation: To be useful to investigation and appeals processes, stored test security information should be quickly and easily available, and access to that information should be limited to authorized individuals in relevant roles.

6 Risks of Online Proctoring

Online proctors and the online proctoring system can actually pose a test security threat. Care must be taken to insulate the testing session and test content from the proctoring system, including from the online proctors.

6.1 Online proctors, as well as on-site proctors, should not attempt to identify test takers.

Explanation: Online proctors are not able to detect falsified identification documents reliably (see points 1.1 and 1.2). Identification documents can be faked

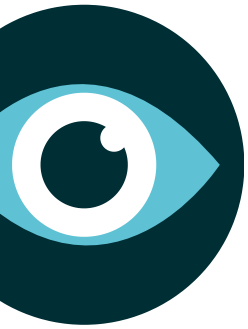
easily. The quality of these documents can be so good that online proctors cannot determine their validity, especially when viewed through a webcam. There are services on the internet that will provide such documents to a test taker for a nominal fee.

6.2 Online proctors should never be able to view test content.

Explanation: Online proctoring systems often use popular off-the-shelf "remote-in" software to grant the proctor the ability to view the test taker's screen. While this access is described as a security measure itself (to make sure that the test takers are not accessing prohibited resources such as external websites), it in fact increases the security risks. It can allow the proctor to potentially coach the test taker or to harvest and then share the content that they see on the exam. Therefore, proctors should never be permitted to view test content.[4]

6.3 Recording an unproctored online testing session for later review should be used sparingly, if at all.

Explanation: "Record and review" is usually offered by online proctoring vendors as a lower-cost option. The main test security value of the "record and review" option is a deterrent measure, but it is a poor deterrent. It is likely that such a review never happens and that test takers realize that fact. Test security, like any other type of security, requires the immediate detection of security incidents, and the opportunity to quickly intervene and respond to any observed incident. Neither of those is possible with "record and review" online proctoring.



6.4 Use of eye movement technology to detect cheating should not be used.

Explanation: There is no evidence today that a test taker's eye movements during an exam indicate that cheating is happening. Excessive movement of other parts of the body might be more relevant, such as getting up and leaving the testing environment or picking up a cell phone or notepad. Test takers move their eyes for many reasons that have nothing to do with cheating. It represents a serious business risk to a program to make test security decisions during a test based on eye movement detection technology.

6.5 Online proctors or an online proctoring system should not be relied upon for the sole test security solution.

[4] This practice is often defended by online proctoring vendors as mimicking the conditions of in-person proctoring. (A proctor in a test center is able to walk around and view test taker screens.) However, this is a security risk in test centers as well, and should not be mimicked by online proctoring, particularly when technology can be used to prevent it.

Explanation: It is a risk to a testing program to rely on any single test security method (see the "Threats and Test Security Solutions" section of this paper). This is particularly relevant with any form of proctoring. Proctoring in general, including online proctoring, is a mediocre test security solution. By itself, it is unable to prevent, detect, or deter most test security threats. Some threats (e.g., the theft of test content using hidden cameras or cheating using pre-knowledge of test content) are and will always be completely hidden from proctors (learn more in this document). No online proctoring vendor, nor their clients, should ever recommend online proctoring as the sole test security solution.

7 Enhancing Online Proctoring through Better Overall Security Practices

Online proctoring is an important contribution to test security. Its effectiveness should be enhanced when possible.

7.1 Assignment of online proctors to monitor test takers should be as random as possible.

Explanation: Proctors, including online proctors, should be randomly assigned to monitor each test taker. This random process helps proctors to be objective as they go about their test security activities, and it eliminates the possibility of bribery or collusion.

7.2 The test security activities of online proctors should be enhanced by technology whenever possible.

Explanation: Human eyes and ears are not as sensitive as we would like them to be, and that sensitivity is often dulled by the insertion of webcams and microphones during the testing process. It is helpful when online proctoring systems can monitor relevant visual movement and excessive audio signals and then alert the online proctor to what has been detected. It isn't just the proctor's senses that can be enhanced in this way. The online proctoring system can be set up to detect inappropriate keystrokes (such as keystrokes used to access prohibited resources or to copy and paste items on the screen). Plus, the online proctoring system can detect unusual response patterns as test takers answer a series of items or patterns that might indicate efforts to cheat or harvest content.

7.3 Testing programs can make online proctors more effective by setting up a comprehensive security system where most test security threats are prevented prior to the test administration event.

Explanation: Online proctors, like on-site proctors, are being asked today to deal with test security threats that are impossible for them to detect (e.g., surreptitious cheating and the use of hidden cameras to harvest test content). Proctors should only be asked to deal with those security threats for which they can be effective (learn more about the effective roles and responsibilities of proctors in this white paper).

Today, testing programs have many more test security tools to protect themselves before ever involving proctors. In the past, the use of large numbers of equivalent test forms served to confound test thieves. Randomization of test content, such as the order of items, will prevent the use of "answer keys" and traditional cheating by copying from a neighboring test taker. Recently, new test designs (e.g., using computerized adaptive testing, pulling items in real time from a very large pool, or other dynamic item content rendering approaches) will provide each test taker with a unique test form. Unique forms make the theft of items unprofitable for the thief as well as the cheater (you can learn more about randomization and unique forms in this article). With such threats neutralized, online proctors can be easily trained and provided tools to help deal with the few threats that remain. For example, online proctors should be able to easily detect if another person is in the room helping the test taker.

7.4 Online proctors should be trained broadly in test security and specifically in those test security activities relevant to their role as proctors.

Explanation: Today, few, if any, proctors are trained in test security. Yet they play an important role in the entire process. It is important for them to understand how what they do fits within the entire scheme of test security. In this way, they can be better prepared to expect particular threats and be better able to deal with those threats when they are encountered.

7.5 Evidence should be provided on the effectiveness of online proctoring.

Explanation: Casual statements about or traditional acceptance of proctoring, including online proctoring, is certainly not sufficient anymore. The stakes are too high, and changes due to advancing technology are occurring too rapidly to simply accept any form of proctoring at face value. It isn't difficult to conduct scientific research and provide evidence that, through online proctoring, the risk from test security threats has reduced or been eliminated altogether (read more in this case study). The online proctor's role in those outcomes can be determined and extolled. Such research will also lead to recommendations as to what is not working well and how it can be modified. It is too dangerous to accept the effectiveness of online and on-site proctoring on the basis of faith or tradition.

CONCLUSION

These guidelines provide a set of objective and practical standards for securely administering tests using online proctors. They focus solely on guidelines related to test security and have been written to maximize online proctoring's impact on the three categories of solutions that prevent, detect/react to, and deter cheating and theft.

While online proctoring contributes to the overall effectiveness of a test security plan, proctoring is not a comprehensive test security solution on its own. Any security plan that includes the use of online proctoring should maximize its effectiveness by combining the three categories of solutions that prevent, detect/react, and deter cheating and theft.

When determining which security solutions to implement, including proctoring, a testing program and/or services provider must prioritize the available solutions that address threats posing the highest risks to the individual program. A firm grasp on the threats and risks is necessary to understand the standards being proposed in this document and is the starting place for all effective test security efforts.