Assessment of Greenwood County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Greenwood County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDOE Unity Image Configuration...</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Greenwood county as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Sergeant J Grover Carlton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the county, 2) the Unity Workstation configuration, and 3) the data-transfer methodologies specific to Greenwood county. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered [redacted]. It was later discovered that [redacted]. While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

   Nothing Significant to Report

2. Unity Workstation Configuration Assessment

   2.1 Threat Level: High

   Description: [Redacted]

   Impact: [Redacted]

   Recommendation: [Redacted]

3. Data-Transfer Methodologies Assessment

   3.1 Threat Level: High

   Description: [Redacted]

   Impact: [Redacted]

   Recommendation: [Redacted]
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", "Escort Name" (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=\|{}[]:;"'<>,.?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Hampton County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Hampton County Elections & Voter Registration Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 20, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Hampton County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Second Lieutenant Leo Pate III. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Hampton County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 “high” vulnerabilities, and 1 “medium” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered . It was later discovered that . While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your County should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your County again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

Nothing significant to report.

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description: ...

Impact: ...

Recommendation: ...

2.2 Threat Level: Medium

Description: ...

Impact: ...

Recommendation: ...
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- **Enforce password history** = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- **Maximum password age** = 120 days
  - This will set mandatory password changes every 120 days
- **Minimum password age** = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- **Minimum password length** = 14 characters
  - This will force any password to be at least 14 characters long
- **Password must meet complexity requirements** = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- **Store password using reversible encryption** = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-=\|{}:;"'<,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user's attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

- Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaverer after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Horry County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Horry County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 16
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Horry County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Warrant Officer 1 James Billingsley. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Horry County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered __________. It was later discovered that __________. While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description: 

Impact: 

Recommendation: 

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description: 

Impact: 

Recommendation: 

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description: [Blank]

Impact: [Blank]

Recommendation: [Blank]

• [Blank]
• [Blank]
• [Blank]
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County’s portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- **Enforce password history** = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- **Maximum password age** = 120 days
  - This will set mandatory password changes every 120 days
- **Minimum password age** = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- **Minimum password length** = 14 characters
  - This will force any password to be at least 14 characters long
- **Password must meet complexity requirements** = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- **Store password using reversible encryption** = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=~\{}\[]:;"'<,/>).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember” could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Jasper County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Jasper County Elections & Voter Registration Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 20, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Jasper County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Second Lieutenant Leo Pate III. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Jasper County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 “critical” vulnerability, and 4 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your County should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your County again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High
Description: 
Impact: 
Recommendation: 

1.2 Threat Level: High
Description: 
Impact: 
Recommendation: 

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical
Description: 
Impact: 
Recommendation:

•
•
•

2.2 Threat Level: High

Description:

Impact:

Recommendation:

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Recommendation:

•

•

•

•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

**Passwords**

**Password Policy**

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_+-=`|(){}\[\]:;"'<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

**Password Construction**

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-_=\`{|}[\]:;"'<>?,/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).

Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*%!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.

*(NOTE: Do not use this specific example as passwords!)*
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Kershaw County’s Election Information Security Posture

Requested by: Executive Director – South Carolina State Election Commission
Prepared for: Kershaw County Voter Registration Department
Conducted by: South Carolina National Guard Defensive Cyber Operations Element
October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td><strong>Key Findings</strong></td>
<td></td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td><strong>Other Observations and Recommendations</strong></td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 21, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Kershaw County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Kershaw County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 "critical" vulnerability and 2 “high” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered... While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

Nothing Significant to Report

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description:

Impact:

Recommendation:

•

•

•

2.2 Threat Level: High

Description:
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description: 

Impact:  

Recommendation: 

•  
•  
•  
•  
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have
any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+|~=-\`{}][;:"'<>,.$/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!*ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
• When maximum event log size is reached = Do not overwrite events (Clear logs manually)

Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This report and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Lancaster County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Lancaster County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 20, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Lancaster County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Lancaster County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 "critical" vulnerability and 1 “high” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered It was later discovered that While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

Nothing Significant to Report

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description:

Impact:

Recommendation:

•

•

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:
Impact:

Recommendation:

- 
- 
- 
-
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from
County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered  
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days  
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days  
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters  
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled  
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:";'<>?,./
- Store password using reversible encryption = Disabled  
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=`|{}[]:;"'<>,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.

- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*!&$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.

**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

• Account Lockout Duration = 45 Minutes
• Account Lockout Threshold = 5 invalid login attempts
• Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

• Audit account logon events = Success and Failure
  o This records every attempt at trying to log onto the computer
• Audit account management = Success and Failure
  o This records attempts to create, rename or disable users and groups and account passwords
• Audit policy change = Failure only
  o This records attempts to modify the audit policy and other security settings that were previously set
• Audit privilege use = Failure only
  o This records each time a user invokes a “privileged” operation on the computer such as a Backup or Restore operation
• Audit object access = Failure only
  o This records users who attempt to open or view files
• Audit logon events = Success and Failure
  o This records the result of event logon attempt
Audit system events = Success and Failure
  o This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)

Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.
Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.

Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features
include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a
computer could become compromised by a malicious person increases. It is a good practice to disable all
features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the
computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer
itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability
of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this
capability back). This can normally be done with a Philips head screwdriver but different models of computers
will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for
assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no
representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any
system or systems examined. The findings and recommendations included in this report should be reviewed and only
implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the
information provided is strictly at your own risk.
Assessment of Laurens County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Laurens County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 24, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Laurens County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Chief Warrant Officer 2 Stephen Szabo. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Laurens County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment
   Nothing Significant to Report

2. Unity Workstation Configuration Assessment
   2.1 Threat Level: High
      Description: ...
      Impact: ...
      Recommendation: ...

3. Data-Transfer Methodologies Assessment
   3.1 Threat Level: High
      Description: ...
      Impact: ...
      Recommendation: ...
Recommendation: [Redacted]
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstation(s) that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
### Annex A: Unity Image Configuration Recommendations

*(Passwords, Account Lockout, Security Auditing, and Other Good Practices)*

*(When implementing these changes ensure that you do the same process on each workstation)*

#### Passwords

##### Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- **Enforce password history** = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- **Maximum password age** = 120 days
  - This will set mandatory password changes every 120 days
- **Minimum password age** = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- **Minimum password length** = 14 characters
  - This will force any password to be at least 14 characters long
- **Password must meet complexity requirements** = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: !@#$%^&*()-_=+\|{\}[;"'<>,.?/
- **Store password using reversible encryption** = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

##### Password Construction

**Strong passwords have the following characteristics:**

- Contain **at least** 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain **at least** one number (for example, 0-9).
- Contain **at least** one special character (for example, !$%^&*()-_=+\|{\}[;"'<>,.?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
Other Recommended Best Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screensaver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L,” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This report and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Lee County’s
Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Lee County Elections Office
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td><strong>Key Findings</strong></td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>6</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 21, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Lee County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Lee County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 "critical" vulnerabilities and 4 “high” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered  

It was later discovered that  

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description:  

Impact:  

Recommendation:  

1.2 Threat Level: Critical

Description:  

Impact:  

Recommendation:  
2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

• [Redacted]
• [Redacted]
• [Redacted]

2.2 Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]
2.3 Threat Level: High
Description: 
Impact: 
Recommendation: 

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High
Description: 
Impact: 
Recommendation: 
• 
• 
• 
•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDCCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDCCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDCCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDCCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDCCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDCCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDCCOE. It is the SCMDCCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have
any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_+-=\|(){}:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=\|{}:;"'<>,.?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!*ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Lexington County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Lexington County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 16
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Lexington County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Warrant Officer 1 James Billingsley. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Lexington County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment
   Nothing Significant to Report

2. Unity Workstation Configuration Assessment
   2.1
   Threat Level: High
   Description:
   Impact:
   Recommendation:

   2.2
   Threat Level: High
   Description:
   Impact:
   Recommendation:
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:

•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization's overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: **Unity Image Configuration Recommendations**  
(*Passwords, Account Lockout, Security Auditing, and Other Good Practices*)  
(*When implementing these changes ensure that you do the same process on each workstation*)

**Passwords**

**Password Policy**

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered  
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days  
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days  
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters  
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled  
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:";'<>?,./
- Store password using reversible encryption = Disabled  
  - This will not store passwords using a weaker encryption method which makes it easier to crack

**Password Construction**

**Strong passwords have the following characteristics:**

- Contain **at least** 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain **at least** one number (for example, 0-9).
- Contain **at least** one special character (for example, !$%^&*_-+=`|(){}[]:";'<>?,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
**Contain work-related information such as building names, system commands, sites, companies, hardware, or software.**

- Contain number patterns such as aabbcc, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of "Welcome123" "Password123" "Changeme123"

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screensaver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Marion County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Marion County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 16
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Marion County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Warrant Officer 1 James Billingsley. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Marion County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "critical" vulnerabilities and 2 “high” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered It was later discovered that While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: Critical

Description:

Impact:

Recommendation:

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description:

Impact:

Recommendation:
2.2

Threat Level: Critical

Description:

Impact:

Recommendation:

3. Data-Transfer Methodologies Assessment

3.1

Threat Level: High

Description:

Impact:

Recommendation:

•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<,>.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=\{|\}][\":;'<>?,/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Marlboro County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Marlboro County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element
October 31, 16
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td><strong>Key Findings</strong></td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Marlboro County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Warrant Officer 1 James Billingsley during this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Marlboro County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 4 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description:

Impact:

Recommendation:

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description:

Impact:

Recommendation:

2.2 Threat Level: High
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:

• 

• 

• 

•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-_=+\{};"'<,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
**Other Good Practices**

**Use of Administrator Account vs Standard User Account**

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

**Disabling Built-In Accounts and/or Deleting Unneeded Accounts**

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of McCormick County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: McCormick County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element
October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td> Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td> Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td> Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMiDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 25, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within McCormick County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Chief Warrant Officer 2 Stephen Szabo. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to McCormick County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered [redacted]. It was later discovered that [redacted]. While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

Nothing Significant to Report

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]
Recommendation:
Other Observations and Recommendations

The Elections Director, Katy Smith, is a subject matter expert on the election process. She articulated the process from memory without the help of notes or resources. She holds accountability for the election process and demonstrated security practices. Her staff also explained their roles and responsibilities relating to the election process without the help of notes or resources. Mrs. Smith produced written policies and procedures outlining the entire voter registration and elections process, to include roles and responsibilities of the department. Aiken County’s techniques, policies and procedures could be considered for use as an example of what other Counties could be doing as they begin moving to improve their security posture.

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed.
at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstation(s) that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County’s portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:";'<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*())~-=\}{]:";'<>?,/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

Contain common words spelled backward, or preceded or followed by a number (for example, terces, secretI or lsecret).

Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(Note: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&&!ThisMorning!).

(Note: Do not use this specific example as passwords!)

Password Protection

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
Other Recommended Best Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Newberry County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Newberry County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Executive Summary</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Findings</strong></td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>6</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>7</td>
</tr>
<tr>
<td><strong>Other Observations</strong></td>
<td>9</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>11</td>
</tr>
</tbody>
</table>
Executive Summary

On October 19, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Newberry county as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Sergeant J. Grover Carlton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the county, 2) the Unity Workstation configuration, and 3) the data-transfer methodologies specific to Newberry county. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 “critical” vulnerability, 5 “high” vulnerabilities, and 4 “medium” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1

Threat Level: High

Description: 

Impact: 

Recommendation: 

1.2

Threat Level: High

Description: 

Impact: 

Recommendation: 

1.3
Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

1.4

Threat Level: Medium

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

1.5

Threat Level: Medium

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]
1.6

Threat Level: Medium

Description: 

Impact: 

Recommendation: 

1.7

Threat Level: Medium

Description: 

Impact: 

Recommendation: 

2. Unity Workstation Configuration Assessment

2.1

Threat Level: Critical

Description: 

Impact: 

Recommendation: 

2.2  
Threat Level: High 

Description: 

Impact: 

Recommendation: 

3. Data-Transfer Methodologies Assessment  

3.1  
Threat Level: High 

Description: 

<table>
<thead>
<tr>
<th>Impact:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
</tr>
<tr>
<td>I</td>
</tr>
<tr>
<td>I</td>
</tr>
<tr>
<td>I</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recommendation:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
</tr>
<tr>
<td>I</td>
</tr>
<tr>
<td>I</td>
</tr>
</tbody>
</table>
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important...
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:";'<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-_+|~=`\{}[]:'"<>?,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(Note: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(Note: Do not use this specific example as passwords!)

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.

Use of Screensaver Password
It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Oconee County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Oconee County Voter Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td><strong>Key Findings</strong></td>
<td></td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td><strong>Other Observations and Recommendations</strong></td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 17, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Oconee as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Oconee County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 "critical" vulnerability, 2 “high” vulnerabilities, and 2 “medium” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: Medium

Description: 

Impact: 

Recommendation: 

1.2 Threat Level: Medium

Description: 

Impact: 

Recommendation: 

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description: 

Impact: 

Recommendation: 

UNCLASSIFIED//FOUO
Impact:

Recommendation:

2.2 Threat Level: High

Description:

Impact:

Recommendation:

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT
personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

When implementing these changes ensure that you do the same process on each workstation

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*(_+-=\{}:;"'<,?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user's attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user's password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Orangeburg County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Orangeburg County Elections & Voter Registration Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>5</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 18, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Orangeburg County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Second Lieutenant Leo Pate III. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Orangeburg County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "high" vulnerabilities, and 1 “medium” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your County should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your County again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

Nothing significant to report.

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description: [Redacted]

Impact: [Redacted]
Recommendation:

- 
- 
- 
-
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County’s portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!#$%^&*-_+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:\;"'<>,.?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Pickens County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Pickens County Registration and Elections Commission
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>6</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 17, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Pickens County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Pickens County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 “critical” vulnerabilities, 3 "high" vulnerabilities and 1 “medium” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment
1.1 Threat Level: Medium
Description: 
Impact: 
Recommendation: 

2. Unity Workstation Configuration Assessment
2.1 Threat Level: Critical
Description: 
Impact: 
Recommendation: 


2.2

Threat Level: Critical

Description:

Impact:

Recommendation:

2.3

Threat Level: High

Description:

Impact:

Recommendation:

2.4

Threat Level: High

Description:
3. Data-Transfer Methodologies Assessment

3.1 [Redacted]

Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*(_+-=\{|}\):';<>?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”
You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases
A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection
• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This report and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Richland County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Richland County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 19, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Richland county as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Sergeant J Grover Carlton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the county, 2) the Unity Workstation configuration, and 3) the data-transfer methodologies specific to Richland county. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 “high” vulnerabilities and 1 "medium" vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered [redacted]. It was later discovered that [redacted]. While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description: [Redacted]
Impact: [Redacted]
Recommendation: [Redacted]

1.2 Threat Level: Medium

Description: [Redacted]
Impact: [Redacted]
Recommendation: [Redacted]

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description: [Redacted]
Impact:

Recommendation:

2.2

Threat Level: High

Description:

Impact:

Recommendation:

3. Data-Transfer Methodologies Assessment

3.1

Threat Level: High

Description:

Impact:

Recommendation:
Recommendation:

• ...
• ...
• ...
• ...
• ...

UNCLASSIFIED//FOUO
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is
important to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: **Unity Image Configuration Recommendations**

*(Passwords, Account Lockout, Security Auditing, and Other Good Practices)*

*(When implementing these changes ensure that you do the same process on each workstation)*

### Passwords

#### Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- **Enforce password history = 12 passwords remembered**
  - This will not allow the last 12 passwords to be reused
- **Maximum password age = 120 days**
  - This will set mandatory password changes every 120 days
- **Minimum password age = 3 days**
  - This will not allow a password to be changed until 3 days after the last password change
- **Minimum password length = 14 characters**
  - This will force any password to be at least 14 characters long
- **Password must meet complexity requirements = Enabled**
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- **Store password using reversible encryption = Disabled**
  - This will not store passwords using a weaker encryption method which makes it easier to crack

#### Password Construction

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*(_-+|~-=\{\}:;''<>?./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, ”This May Be One Way To Remember” could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Saluda County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Saluda County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element
October 31, 16
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 25, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Saluda County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Warrant Officer 1 James Billingsley. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Saluda County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment
Nothing Significant to Report

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High
Description:
Impact:
Recommendation:

2.2 Threat Level: High
Description:
Impact:
Recommendation:
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*-+=\`|(){}[]:";'<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-_=\`|(){}[]:";'<>?,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

(NOTE: Do not use this specific example as passwords!)

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.

(NOTE: Do not use either of these specific examples as passwords!)

UNCLASSIFIED//FOUO
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Spartanburg County's Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Spartanburg County Voter Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td><strong>Key Findings</strong></td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>6</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCNGDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 17, 2016, the South Carolina National Guard Defensive Cyber Operations Element (SCNGDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Spartanburg County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCNGDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Spartanburg County. All vulnerabilities discovered within these three areas, as identified by the SCNGDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCNGDCOE’s recommendation in mitigating that vulnerability.

The SCNGDCOE’s rapid assessment resulted in 1 "critical" vulnerability, 3 “high” vulnerabilities, and 1 “medium” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCNGDCOE discovered [redacted] While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCNGDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCNGDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCNGDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCNGDCOE.
Key Findings

1. Physical Security Assessment

1.1 [Redacted]

Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]

1.2 [Redacted]

Threat Level: High

Description: [Redacted]

Impact: [Redacted]

Recommendation: [Redacted]
2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical
Description:

Impact:

Recommendation:

2.2 Threat Level: Medium
Description:

Impact:

Recommendation:
3. Data-Transfer Methodologies Assessment

3.1

Threat Level: High

Description:  

Impact:  

Recommendation:  

with this method

Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization's overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCNGDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", "Escort Name" (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badge to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCNGDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCNGDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCNGDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCNGDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCNGDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCNGDCOE. It is the SCNGDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT
personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCNGDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County’s portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCNGDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCNGDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+="||{}[]:'"<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*_-+="||{}[]:'"<>?,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret 1 or lsecret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password Tmb!w2R! or another variation.

**(NOTE: Do not use either of these specific examples as passwords!)**

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*!$ThisMorning!).

**(NOTE: Do not use this specific example as passwords!)**

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, coworkers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user's attempt to "log in" on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to "crack" or guess a user's password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a "privileged" operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
**Other Good Practices**

**Use of Administrator Account vs Standard User Account**

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

---

**Disabling Built-In Accounts and/or Deleting Unneeded Accounts**

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.
Assessment of Spartanburg County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Spartanburg County Voter Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element
October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>6</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 17, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Spartanburg County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Spartanburg County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 "critical" vulnerability, 3 “high” vulnerabilities, and 1 “medium” vulnerability that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description:

Impact:

Recommendation:

1.2 Threat Level: High

Description:

Impact:

Recommendation:
2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description: 

Impact: 

Recommendation: 

2.2 Threat Level: Medium

Description: 

Impact: 

Recommendation: 

UNCLASSIFIED//FOUO
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations
(Passwords, Account Lockout, Security Auditing, and Other Good Practices)
(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=|\{}[]:;"'<,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”) 
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extend the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Sumter County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Sumter County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 24, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Sumter County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Chief Warrant Officer 2 Stephen Szabo. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Sumter County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered

It was later discovered that

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
**Key Findings**

1. Physical Security Assessment

   **Nothing Significant to Report**

2. Unity Workstation Configuration Assessment

   2.1 **Threat Level:** High

   **Description:**

   **Impact:**

   **Recommendation:**

3. Data-Transfer Methodologies Assessment

   3.1 **Threat Level:** High

   **Description:**

   **Impact:**

   **Recommendation:**
Recommendation:

- 
- 
- 
-
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure.

The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstation(s) that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()_+-=~\{|}';"<>?,./).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
When maximum event log size is reached = Do not overwrite events (Clear logs manually)

**Other Recommended Best Practices**

**Use of Administrator Account vs Standard User Account**

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

- Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extend the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This report and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Union County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Union County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>6</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>8</td>
</tr>
</tbody>
</table>
Executive Summary

On October 24, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Union County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Chief Warrant Officer 2 Stephen Szabo. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Union County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 3 "high" vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment Summary

1.1 Threat Level: High

Description:

Impact:

Recommendation:

2. Unity Workstation Configuration Assessment

2.1 Threat Level: High

Description:

Impact:

Recommendation:
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", "Escort Name" (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important
to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County’s cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

**Passwords**

**Password Policy**

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- **Enforce password history = 12 passwords remembered**
  - This will not allow the last 12 passwords to be reused
- **Maximum password age = 120 days**
  - This will set mandatory password changes every 120 days
- **Minimum password age = 3 days**
  - This will not allow a password to be changed until 3 days after the last password change
- **Minimum password length = 14 characters**
  - This will force any password to be at least 14 characters long
- **Password must meet complexity requirements = Enabled**
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: !@#$%^&*_-+=`|(){}[]:'",.<>?/
- **Store password using reversible encryption = Disabled**
  - This will not store passwords using a weaker encryption method which makes it easier to crack

**Password Construction**

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()-_=+\|{}[]:;'<?,/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, “This May Be One Way To Remember” could become the password TmB1w2R! or another variation.

(Note: Do not use either of these specific examples as passwords!)

Passphrases

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!ThisMorning!).

(Note: Do not use this specific example as passwords!)

Password Protection

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
Account Lockout

Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)
Other Good Practices

Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of Williamsburg County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: Williamsburg County Registration and Elections Department
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 24, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within Williamsburg County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to Williamsburg County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information; 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 2 "critical" vulnerabilities and 3 “high” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered [Redacted].

It was later discovered that [Redacted].

While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: Critical

Description:

Impact:

Recommendation:

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description:

Impact:

Recommendation:
2.2 Threat Level: High
Description:
Impact:
Recommendation:

2.3 Threat Level: High
Description:
Impact:
Recommendation:
3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description:

Impact:

Recommendation:

•
•
•
•
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE's recommendation that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE's recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from
County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`|(){}[]:;"'<>,.?/
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

**Strong passwords have the following characteristics:**

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*(_+\"{};"<>?/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

**Poor, or weak, passwords have the following characteristics:**

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

- Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
- User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
- All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
- All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords will not be revealed on questionnaires or security forms.
- Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
- Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- If your password is suspected as being compromised, you must report the incident and change all passwords.

**Account Lockout**
Account Lock Out Policy

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

Security Auditing

Auditing Policy

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

Managing Logs

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
- When maximum event log size is reached = Do not overwrite events (Clear logs manually)

Other Good Practices
Use of Administrator Account vs Standard User Account

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

Disabling Built-In Accounts and/or Deleting Unneeded Accounts

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.

Use of Screensaver Password
It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

*It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.*

**Disabling Unneeded/Unused Features**

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This report and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.
Assessment of York County’s Election Information Security Posture

Requested By: Executive Director - South Carolina State Election Commission
Prepared For: York County Elections Office
Prepared By: South Carolina National Guard Defensive Cyber Operations Element

October 31, 2016
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Key Findings</td>
<td>4</td>
</tr>
<tr>
<td>Physical Security Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Unity Workstation Configuration Assessment</td>
<td>4</td>
</tr>
<tr>
<td>Data-Transfer Methodologies Assessment</td>
<td>5</td>
</tr>
<tr>
<td>Other Observations and Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Annex A: SCMDDCOE Unity Image Configuration Recommendations</td>
<td>9</td>
</tr>
</tbody>
</table>
Executive Summary

On October 20, 2016, the South Carolina Military Department Defensive Cyber Operations Element (SCMDDCOE) conducted a rapid vulnerability assessment on the election processes, procedures, and devices within York County as requested by the South Carolina State Election Commission. This rapid assessment was conducted by Master Sergeant Ricky Chapman (lead) and Staff Sergeant Marquis Benton. During this rapid assessment, the SCMDDCOE focused on three areas. These areas were 1) the physical security of the election materials for the County, 2) the Unity workstation configuration, and 3) the data-transfer methodologies specific to York County. All vulnerabilities discovered within these three areas, as identified by the SCMDDCOE, will be annotated in this report as either “critical”, “high”, or “medium” and will provide the following information: 1) the description of the vulnerability, 2) the impact this vulnerability could have if exploited, and 3) the SCMDDCOE’s recommendation in mitigating that vulnerability.

The SCMDDCOE’s rapid assessment resulted in 1 "critical" vulnerability and 3 “high” vulnerabilities that require immediate attention. These vulnerabilities are outlined in the ‘Key Findings’ section under its respective area.

When conducting this rapid assessment, the SCMDDCOE discovered [Redacted]. It was later discovered that [Redacted]. While there is a significant number of security controls that could be implemented to better secure the Unity workstation, due to short amount of time between the receipt of this report and the upcoming national election, the SCMDDCOE decided to create an annex to the final report that lists specific actions that can be implemented with a low risk to the disruption of operations.

It is important to note that the SCMDDCOE recommendations included in this report should be implemented after careful consideration from all stakeholders. Any changes implemented due to these recommendations should be made in accordance with the South Carolina State Election Commission’s change management and configuration control policies and procedures. Changes made without due care and consideration could render a system inoperable. Functional testing should always be included in your change management plan. Given the short amount of time between receipt of this report and the upcoming national election, it may not be prudent to implement these changes before the event. Your county should make a risk-based determination based on its abilities, resources, and circumstances.

The SCMDDCOE welcomes any feedback or other questions and concerns regarding this report or its findings and we look forward to working with your county again. Should you have any questions, comments, or concerns, please feel free to reach out the SCMDDCOE.
Key Findings

1. Physical Security Assessment

1.1 Threat Level: High

Description:

Impact:

Recommendation:

2. Unity Workstation Configuration Assessment

2.1 Threat Level: Critical

Description:

Impact:

Recommendation:

•
2.2 Threat Level: High

Description: [redacted]

Impact: [redacted]

Recommendation: [redacted]

3. Data-Transfer Methodologies Assessment

3.1 Threat Level: High

Description: [redacted]

Impact: [redacted]

Recommendation: [redacted]
Other Observations and Recommendations

One of the greatest and widespread vulnerabilities presenting risk to an organization’s overall cybersecurity posture is unauthorized personnel obtaining physical access to secure areas that contain sensitive IT equipment. Best practices for mitigating these risks are 1) establishing a physically secure area for the storage of sensitive IT equipment and 2) limiting access to this area to authorized personnel only. The Counties can establish a physically secure area by utilizing physical access controls (e.g. locks, walls, cameras, etc.) and accountability controls (e.g. limiting the number of personnel who possess a key). It is the SCMDDCOE’s recommendation that a visitor log and physical access control log, used to track persons entering the physically secure areas where sensitive IT equipment is located, be established. An access control log, used in conjunction with a CCTV camera or door chime system, can be used to help implement controlled access and aid follow-up investigations if necessary. The Access Control Log should consist of a "Date", "Time of Access", "Name", "Reason for Visit", “Escort Name” (if needed) and "Time of Exit" field. Some circumstances require sensitive IT equipment to be stored and used in less secure areas or during events where large volumes of foot traffic is expected. A common mitigation strategy implemented in cases like these is for authorized personnel to wear distinctive apparel or badging to distinguish themselves from those around them, and make it clearly visible when unauthorized persons may attempt to approach and access sensitive IT equipment. This helps authorized personnel easily identify and preempt attempted access by unauthorized parties. It is also the SCMDDCOE’s recommendation, that every County consider which physical access controls/mitigation measures best meet their circumstances and implement appropriate measures to limit and track personnel accessing sensitive IT systems and secure areas where election materials and IT equipment are stored and/or used.

Due to time constraints, the SCMDDCOE’s rapid assessments with the Counties were primarily focused on several key components of the election infrastructure and process. Unfortunately, there was not enough time to establish expressed, written agreements and permission to access and examine county-owned workstations used in the election process. This impacted the SCMDDCOE’s ability to observe and assess risks presented by the county-owned workstation(s) used as election infrastructure. The SCMDDCOE identified the workstation(s) that had been designated for these roles and confirmed whether they are county-owned workstations and subject to County IT management, but did not have an opportunity to assess the risks presented by their configuration & confirm whether appropriate security controls were in place. This presents an open risk, because without assessing these workstations—the SCMDDCOE was not able to verify that possible start and end-points of relevant election data have the proper controls in place to safeguard this information. While the County may have placed proper controls on the workstation(s), it has not been verified or the risk accurately assessed at this point by the SCMDDCOE. It is the SCMDDCOE’s recommendation that an in-depth follow-on assessment be conducted on the county-owned workstations that are performing this function, after expressed, written permission from the Counties can be obtained. It is also imperative that appropriate IT support personnel be present for the in-depth assessment to answer any technical questions, observe first-hand any risks that may be identified and to ensure they understand recommended mitigation or remediation measures.

In many Counties, designated IT personnel were not present (or the County did not have
any IT support available) during the rapid assessment. While this may not apply to this County, it is important to express how crucial it is that the County Election Commissioners have IT support from County IT personnel, a third-party entity (with County approval), or from the State of South Carolina. It is the SCMDDCOE’s recommendation that designated IT personnel be available during any assessment to ensure a better understanding of the risks being assessed, any discrepancies identified and potential issues with their County's cybersecurity posture. It would also ensure IT personnel’s immediate awareness of any critical findings and the recommended mitigation actions from those conducting the assessment. This will enable a timelier resolution which subsequently, improving the security posture for the County's portion of South Carolina’s election infrastructure.

Within various Counties, no official documented policies or procedures detailing specific rules that must be adhered to, could be presented to the SCMDDCOE. While the County Election Officials participating in the assessment could verbally provide specific rules and procedures in answering our hypothetical questions, they could not provide written documentation. It is the SCMDDCOE’s recommendation that Counties closely re-examine their current policies and procedures and formally document them. Documented policies should state exactly what is expected (e.g. rules pertaining to a specific function) across the domain of the County Election’s Office; documented procedures should establish the standard way for how things are done to implement policy. This will aid in identifying possible problems in the process, resulting in more secure policies and procedures being implemented across South Carolina. Good policies and procedures consist of an “Overview,” “Purpose,” “Scope,” the “Policy” or “Procedure” (depending which one is being drafted), “Consequences of Violations,” “Who is Held Responsible,” “Revision History,” “Effective Date,” and “Points of Contact” sections. The final policy and procedure document should be signed and dated under the signature block by the individual who has the authority to implement and enforce it.
Annex A: Unity Image Configuration Recommendations

(Passwords, Account Lockout, Security Auditing, and Other Good Practices)

(When implementing these changes ensure that you do the same process on each workstation)

Passwords

Password Policy

Password policies are used to enforce specific password criteria. You can set these parameters in Windows computers; below are the recommended parameters:

- Enforce password history = 12 passwords remembered
  - This will not allow the last 12 passwords to be reused
- Maximum password age = 120 days
  - This will set mandatory password changes every 120 days
- Minimum password age = 3 days
  - This will not allow a password to be changed until 3 days after the last password change
- Minimum password length = 14 characters
  - This will force any password to be at least 14 characters long
- Password must meet complexity requirements = Enabled
  - This will force three of the following four categories when creating new passwords
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numbers (0 through 9)
    - Special characters: ~!@#$%^&*_-+=`\|(){}[]":;'<>?,./
- Store password using reversible encryption = Disabled
  - This will not store passwords using a weaker encryption method which makes it easier to crack

Password Construction

Strong passwords have the following characteristics:

- Contain at least 14 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !$%^&*()[\]{};":;'<>?,/).
- There are many free password generator tools online that could be utilized to craft your unique passwords but they may be harder to remember. Below is the recommended password generator.

Poor, or weak, passwords have the following characteristics:

- Contain less than 14 characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxvwuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or another phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

*(NOTE: Do not use either of these specific examples as passwords!)*

**Passphrases**

A passphrase is like a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against various password cracking attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*$!*ThisMorning!).

*(NOTE: Do not use this specific example as passwords!)*

**Password Protection**

• Users should not use the same password for any account on any device. There should be a unique password for each account the user has even if the same person is using multiple computers.
• User accounts that have administrator-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access administrator-level privileges.
• All administrator-level passwords should be changed on at least a quarterly (every four months) basis.
• All user-level passwords should be changed at least every six months. The recommended change interval is every four months.
• Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
• Passwords must not be inserted into email messages or other forms of electronic communication.
• Passwords must not be revealed over the phone to anyone.
• Passwords will not be revealed on questionnaires or security forms.
• Password hints will not be used. (If forced to, the hint should be non-descriptive like “Ask IT”)
• Passwords will not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
• Passwords will not be written down and stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
• If your password is suspected as being compromised, you must report the incident and change all passwords.
**Account Lockout**

**Account Lock Out Policy**

Account lockouts are a security feature used to prevent the user’s attempt to “log in” on a computer system before a specified parameter is met. This helps defend against a malicious user or program attempting to “crack” or guess a user’s password. On Windows computers, you can set an Account Lockout Policy to do just that. The following is the recommended parameters that should be set within this policy.

- Account Lockout Duration = 45 Minutes
- Account Lockout Threshold = 5 invalid login attempts
- Reset Account Lockout Counter = 45 Minutes

**Security Auditing**

**Auditing Policy**

Auditing policies are used to enforce specific parameters in regards to recording specific Windows events. These events allow specific records of events that happen on the computer to be recorded which would help later in trying to troubleshoot a problem or see if there are potential compromises. Below are the recommended parameters that should be set in regards to auditing.

- Audit account logon events = Success and Failure
  - This records every attempt at trying to log onto the computer
- Audit account management = Success and Failure
  - This records attempts to create, rename or disable users and groups and account passwords
- Audit policy change = Failure only
  - This records attempts to modify the audit policy and other security settings that were previously set
- Audit privilege use = Failure only
  - This records each time a user invokes a “privileged” operation on the system such as a Backup or Restore operation
- Audit object access = Failure only
  - This records users who attempt to open or view files
- Audit logon events = Success and Failure
  - This records the result of event logon attempt
- Audit system events = Success and Failure
  - This records system shutdown and restart events, log full events and other events that have system-wide significance

**Managing Logs**

By default, logs are stored and only a specified size amount of these logs cumulatively are kept. This overall size is very low by default. These settings can be found in the Windows Logs and Applications and Services Logs within the built-in Windows Event Viewer program. Below are our recommendations in managing these logs:

- Maximum log size = 80,000 KB
When maximum event log size is reached = Do not overwrite events (Clear logs manually)

**Other Good Practices**

**Use of Administrator Account vs Standard User Account**

By default, the Administrator account is enabled on Windows XP. This is a security concern because it is very well known that there is an Administrator account and that it is enabled by default. If discovered that there is a Windows XP workstation on a network, attackers will first target the Administrator account. Therefore, it’s good practice to disable the built-in Administrator account, create a new custom Administrator account and then create new accounts for the Unity’s everyday use that doesn’t have the same privileges as the new Administrator account. Also, it is generally bad practice to use your administrator account for everyday use of a workstation. An administrator account should only be used for things that require such as installing software or creating/deleting/modifying users. The following is a recommendation in how to implement this.

**Disabling Built-In Accounts and/or Deleting Unneeded Accounts**

It is good practice to only allow user accounts to be created on a workstation if they are to be used. Like the good practice listed above, there are built-in accounts that are needed to exist on a Windows workstation for it to function as expected but there are also accounts that are built-in that add a capability that is convenient for the user(s). One of these accounts is the “Guest” account. The “Guest” account is an account that allows guest access to a workstation. It was intended to allow guests (those without user accounts on a workstation) to have access to a workstation to perform basic computer functions like browsing the internet, sending a fax or playing a simple computer game. This account is not password protected, enabled by default, and provides some access to the core files needed for Windows to run. It was later determined that attackers could use this account to compromise the Windows workstation. It is a good practice to disable this user account (you cannot delete this account as it is a built-in account) and any other user accounts you do not use. This will make the possible areas of attacks on the workstation much smaller.
Use of Screensaver Password

It is good practice that only the user logged into the workstation be the only person that uses that workstation. One way that malicious users violate this is if an authorized user steps away from the computer without “locking” it (requiring the use of username and password to regain access), a malicious user can walk up to the workstation and begin using it. One way to mitigate this is to set a screensaver password. If this is set, the computer will go to a screensaver after a specific amount of time and upon trying to regain access to the workstation, the user will be prompted to enter the username and password. Below is how to implement this recommendation:

1. Go to Start → Control Panel → Display.
2. Click on the Screen Saver tab, then choose the screen saver of your choice.
3. Choose to wait 4 minutes.
4. Check the box beside “On resume, password protect.” This will require a password to be entered the next time someone uses the computer.
5. Click on “OK”.

It is highly recommended that when you leave the computer for any amount of time, you should lock it before walking away. Just simultaneously press the Windows button (the key that has the Windows logo) + “L” and the system is automatically locked. A password will be required to resume use of the computer.

Disabling Unneeded/Unused Features

Computers today come with a lot of features that extends the computer’s capabilities. Some of these features include Bluetooth, Wi-Fi, Cameras, Microphones, etc. With each addition of a feature, the number of ways a computer could become compromised by a malicious person increases. It is a good practice to disable all features that aren’t needed or used. Some of these include not only disabling Wi-Fi and Bluetooth within the computer’s operating system but also physically removing the wireless and Bluetooth cards from the computer itself. By removing these cards, you’ve not only disabled this feature but you’ve also eliminated the capability of that computer ever connecting to a wireless signal (unless you plug in an external device that brings this capability back). This can normally be done with a Philips head screwdriver but different models of computers will vary.

This reports and material represents the South Carolina Military Department’s best efforts to respond to a request for assistance by the South Carolina State Elections Commission. The South Carolina Military Departments makes no representations or warranties of any kind, express or implied as to the completeness, accuracy, or reliability of any system or systems examined. The findings and recommendations included in this report should be reviewed and only implemented after careful consideration by the South Carolina State Election Commission. Any reliance on the information provided is strictly at your own risk.