### NIST 800-171 Compliance Criteria

<table>
<thead>
<tr>
<th>NIST 800-171 Requirement</th>
<th>NIST 800-171 Control Objective</th>
<th>Relevant NIST 800-171 Revision / Section Details</th>
<th>Method To Measure Requirement</th>
<th>Compliance Status</th>
<th>Non-Compliance Reason (If Applicable)</th>
<th>Deviation Justification (If Applicable)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3050.1.2</td>
<td>Access Controls</td>
<td>Relevant NIST 800-171 Revision / Section Details</td>
<td>Method To Measure Requirement</td>
<td>Compliance Status</td>
<td>Non-Compliance Reason (If Applicable)</td>
<td>Deviation Justification (If Applicable)</td>
<td>Notes</td>
</tr>
<tr>
<td>3.1 ACCESS CONTROLS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.13.5 - Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).

3.13.6 - Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception). This can include preventing the end of sessions or after a defined alternative physical safeguards.

3.13.7 - Prevent remote devices from establishing non-remote connections with the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.13.8 - Implement system configurations to prevent remote devices from establishing non-remote connections with the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.14.9 - Unauthorized cryptographic mechanisms to prevent unauthorized disclosure of information by unauthorized personnel.

3.14.10 - Prevent unauthorized disclosure of information during transmission.

3.15.6 - Implement system configurations to prevent unauthorized disclosure of information during transmission.

3.15.7 - Implement system configurations to prevent unauthorized disclosure of information during transmission.

3.17.1 - Terminate network connections, associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.19.3 -堵塞菊事数据流的传输, 如: 无线网络和内部网络区域, 同时创建非远程连接 (如, VPN) 与系统、会话或密钥存储安全接通的加密机制。

3.19.4 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.5 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.6 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.7 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.8 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.9 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.

3.19.10 - Secure system configurations require users to re-authenticate to the system from communicating outside that path and with the system from communicating outside that path unless otherwise protected by organization-defined access control policies.