安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
1	身份鉴别	[关键]c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	将HTTP升级为HTTPS。	¥500.00	
2	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥400.00	
3	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥300.00	
4	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制，如仅限制个别终端地址进行访问和管理。	¥200.00	
5	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥100.00	
6	数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	采用校验码技术或密码技术保证重要数据在传输过程中的完整性，相关密码技术符合国家密码管理部门的规定要求。	¥600.00	
7	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥700.00	
8	数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	对系统管理数据、鉴别信息及重要业务数据采用经国家密码主管部门认可的密码技术，保证其在传输过程中数据的保密性。	¥500.00	
9	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥300.00	
10	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥400.00	
11	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥400.00	
12	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥350.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
13	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥280.00	
14	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥400.00	
15	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥300.00	
16	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥400.00	
17	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥500.00	
18	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥600.00	
19	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥600.00	
20	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥300.00	
21	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥400.00	
22	身份鉴别	[重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	配置登录失败处理策略，防止恶意人员暴力破解账户口令；同时配置登录连接超时策略，降低被非授权访问的风险。登录失败策略方面，可根据账户或登录地址	¥400.00	
23	身份鉴别	[关键]c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用加密传输、使用加密协议等措施，防止鉴别信息在传输过程中被窃听。	¥600.00	
24	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥500.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
25	访问控制	[一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	限制超级管理权限账户使用，根据业务需求及安全要求，建立安全管理员、审计管理员、业务功能账户等，并根据业务需要设置各账户的权限，实现管理权限最	¥700.00	
26	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥500.00	
27	安全审计	[一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	将日志发送至日志审计系统对日志进行集中存放或手动保存至硬盘，并确保保存时间能够达到180天以上。	¥200.00	
28	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥300.00	
29	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥400.00	
30	数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	采用校验码技术或密码技术保证重要数据在传输过程中的完整性，相关密码技术符合国家密码管理部门的规定要求。	¥350.00	
31	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥450.00	
32	数据保密性	[关键]a)应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	对系统管理数据、鉴别信息及重要业务数据采用经国家密码主管部门认可的密码技术，保证其在传输过程中数据的保密性。	¥260.00	
33	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥400.00	
34	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥200.00	
35	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥100.00	
36	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥200.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
37	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥200.00	
38	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥500.00	
39	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥300.00	
40	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥500.00	
41	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥600.00	
42	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥700.00	
43	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥200.00	
44	数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能；	建立备份恢复机制，定期对重要数据进行备份以及恢复测试，在出现数据破坏时，可利用备份数据进行恢复。	¥100.00	
45	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥800.00	
46	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥200.00	
47	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥300.00	
48	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥400.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
49	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥200.00	
50	数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能；	建立备份恢复机制，定期对重要数据进行备份以及恢复测试，在出现数据破坏时，可利用备份数据进行恢复。	¥500.00	
51	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥400.00	
52	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥500.00	
53	访问控制	[重要]a)应对登录的用户分配账户和权限；	严格限制默认账户访问权限，对默认账户进行访问控制，如限制远程访问，或锁定系统无用默认账户等。	¥800.00	
54	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥200.00	
55	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥300.00	
56	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥400.00	
57	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥200.00	
58	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥400.00	
59	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥300.00	
60	访问控制	[重要]a)应对登录的用户分配账户和权限；	严格限制默认账户访问权限，对默认账户进行访问控制，如限制远程访问，或锁定系统无用默认账户等。	¥500.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
61	访问控制	[一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	限制超级管理权限账户使用，根据业务需求及安全要求，建立安全管理员、审计管理员、业务功能账户等，并根据业务需要设置各账户的权限，实现管理权限最	¥100.00	
62	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥300.00	
63	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥200.00	
64	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥500.00	
65	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥300.00	
66	身份鉴别	[重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	配置登录失败处理策略，防止恶意人员暴力破解账户口令；同时配置登录连接超时策略，降低被非授权访问的风险。登录失败策略方面，可根据账户或登录地址	¥600.00	
67	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥400.00	
68	访问控制	[重要]a)应对登录的用户分配账户和权限；	严格限制默认账户访问权限，对默认账户进行访问控制，如限制远程访问，或锁定系统无用默认账户等。	¥200.00	
69	访问控制	[重要]c)应及时删除或停用多余的、过期的账户，避免共享账户的存在；	锁定或删除多余账户，并为每个管理员分别创建不同账户，保证不同管理员使用不同账户进行管理。	¥300.00	
70	访问控制	[一般]d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	限制超级管理权限账户使用，根据业务需求及安全要求，建立安全管理员、审计管理员、业务功能账户等，并根据业务需要设置各账户的权限，实现管理权限最	¥400.00	
71	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥600.00	
72	安全审计	[重要]a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	提供安全审计功能，对重要的用户行为和重要安全事件进行审计。	¥300.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
73	安全审计	[一般]b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	重要计算环境设备（包括操作系统、数据库、中间件、网络设备、安全设备、运维终端等）开启安全审计策略，并对安全审计内容进行记录；应用系统应提供安	¥200.00	
74	安全审计	[一般]c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	计算环境设备开启安全审计策略，应用系统提供安全审计功能模块，并对审计记录采取保护措施，如对日志存储介质进行定期备份，或者实时发送至集中审计	¥100.00	
75	安全审计	[一般]d)应对审计进程进行保护，防止未经授权的中断。	计算环境设备开启安全审计功能，限制用户对审计进程的访问，防止非授权人员中断审计进程；有条件采取技术措施对审计进程进行保护，避免受到未经授	¥600.00	
76	入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口；	关闭不必要的服务，关闭不必要的高危端口，仅开启业务所需的服务及端口。	¥500.00	
77	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥400.00	
78	入侵防范	[重要]e)应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	对发现的高风险漏洞进行测评评估，对高风险漏洞进行整改或者加固，如对于应用系统漏洞，由开发单位对漏洞进行代码整改，修复漏洞，无法代码整改情况	¥500.00	
79	入侵防范	[重要]f)应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。	操作系统安装主机层入侵防范软件，对入侵的行为进行检测，并在发生严重入侵事件时提供报警。	¥300.00	
80	恶意代码防范	[重要]应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	在主机操作系统部署防恶意代码检测和清除产品，或配置相应功能可防范恶意代码的产品，如主动可信验证技术产品、白名单管控软件等，及时识别阻断恶意代	¥200.00	
81	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥900.00	
82	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥600.00	
83	数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能；	建立备份恢复机制，定期对重要数据进行备份以及恢复测试，在出现数据破坏时，可利用备份数据进行恢复。	¥100.00	
84	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥200.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
85	数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	系统相关的设备使用热冗余方式部署，如（根据缺失的设备列明细）等，以保证系统高可用性。	¥300.00	
86	剩余信息保护	[重要]a)应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	完善鉴别信息释放或清除机制，确保在执行释放或清除相关操作后，鉴别信息得到完善释放或清除；如WEB应用系统在用户退出后，及时清除浏览器中及应用后	¥600.00	
87	剩余信息保护	[重要]b)应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	计算设备在允许的条件下，使用工具或采取相应措施保证敏感数据所在的存储空间，被释放或再分配给其他用户前得到完全清除。如定期删除Linux操作系统的	¥500.00	
88	身份鉴别	[关键]c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用加密传输、使用加密协议等措施，防止鉴别信息在传输过程中被窃听。	¥700.00	
89	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥500.00	
90	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥600.00	
91	入侵防范	[关键]b)应关闭不需要的系统服务、默认共享和高危端口；	关闭不必要的服务，如telnet服务。	¥500.00	
92	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥100.00	
93	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥600.00	
94	数据完整性	[重要]a)应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	采用校验码技术或密码技术保证重要数据在传输过程中的完整性，相关密码技术符合国家密码管理部门的规定要求。	¥900.00	
95	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥800.00	
96	数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能；	建立备份恢复机制，定期对重要数据进行备份以及恢复测试，在出现数据破坏时，可利用备份数据进行恢复。	¥400.00	

张钢铁 19974406677
张家界蓝盾安防有限责任公司

安全计算环境整改报价清单

日期：2024-5-14

序号	安全控制点	检测项	整改内容	报价	备注
97	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥600.00	
98	数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	系统相关的设备使用热冗余方式部署，如（根据缺失的设备列明细）等，以保证系统高可用性。	¥500.00	
99	身份鉴别	[重要]b)应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	配置登录失败处理策略，防止恶意人员暴力破解账户口令；同时配置登录连接超时策略，降低被非授权访问的风险。登录失败策略方面，可根据账户或登录地址	¥280.00	
100	身份鉴别	[关键]c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用加密传输、使用加密协议等措施，防止鉴别信息在传输过程中被窃听。	¥200.00	
101	身份鉴别	[关键]d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，并且其中一种鉴别技术为密码技术，如：数字证书、动态口令等。	¥430.00	
102	访问控制	[一般]g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	对计算环境资源进行严格划分，并对重要主体和客体进行分级标记，形成完整的资源分级和访问权限控制结构体系，依据安全标记控制主体对信息资源的访问。	¥900.00	
103	入侵防范	[重要]c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	对管理终端的网络地址范围进行限制。	¥400.00	
104	可信验证	[一般]可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检	基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可	¥500.00	
105	数据完整性	[关键]b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数	在重要数据存储时，采用经国家密码主管部门认可的校验技术或密码技术，保证其在存储过程中数据的完整性。	¥600.00	
106	数据备份恢复	[关键]a)应提供重要数据的本地数据备份与恢复功能；	建立备份恢复机制，定期对重要数据进行备份以及恢复测试，在出现数据破坏时，可利用备份数据进行恢复。	¥400.00	
107	数据备份恢复	[重要]b)应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	利用通信网络将重要数据实时传送至备用场地。	¥500.00	
108	数据备份恢复	[关键]c)应提供重要数据处理系统的热冗余，保证系统的高可用性。	系统相关的设备使用热冗余方式部署，如（根据缺失的设备列明细）等，以保证系统高可用性。	¥800.00	
合计		序号1 +序号2 + 序号3 + 序号108		**¥45,000.00**	

张钢铁 19974406677
张家界蓝盾安防有限责任公司