

信息安全应急处理服务资质认证自评表

组织名称		申报级别	
评估时间		评估部门/人员	

序号	要点	条款	需提供证明材料	自评结论		证明材料清单
				符合	不符合	
1	服务技术要求	建立信息安全应急处理服务流程。	按照相关标准建立的信息安全应急处理服务流程,流程图中应包括每个阶段对应的职责、输入输出等。			
2		制定信息安全应急处理服务规范并按照规范实施。	已制定的信息安全应急处理服务规范。			
3	准备阶段	明确客户的应急需求。	应急服务内容,已完成项目中对客户应急需求进行调研分析的证明材料。			
4		了解客户应急预案的内容。	需对客户自身已建立的应急预案的内容进行了解与熟悉(客户应急预案的内容)。			
5		配备有处理网络或信息安全事件的工具包,包括常用的系统命令、工具软件等。	工具包及工具列表			
6		仅二级/一级要求:网络与信息安全事件				

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		工具包中应配备专业技术检测设备。				
7		工具包应定期更新。	工具包更新记录。			
8		配备应急处理服务人员。	服务人员列表、专业资质证书。			
9		对在应急处理服务过程中可能会采取的操作、处理等行为，获得用户的书面授权。	用户出具的书面授权书。			
1		仅二级/一级要求： 在客户应急需求基础上制定应急服务方案。	应急服务方案（模板和实际服务项目方案），应急服务方案中应涵盖客户自身建立的应急预案内容。协助客户建立的应急预案。			
1		仅二级/一级要求： 应急服务方案应涉及客户应急预案的启动与执行。				
1		仅二级/一级要求： 若客户未建立应急预案，可协助客户建立。				
1		仅二级/一级要求： 对工具包实行制度化管理。		工具包管理制度及执行记录。		
1		三级/二级/一级分别要求： 可提供本地 2 小时/本地 1 小时、外地 8 小时/本地 7X24 小时、外地 4 小时应急响应服务能力。	查验服务承诺书、服务合同条款或服务级别协议（结合项目案例）。			
1		仅一级要求： 与客户之间建立安全保密的信息传输渠道。	与客户传输信息时采用可信及保密传输渠道的证明材料。			

序号	要点	条款	需提供证明材料	自评结论		证明材料清单
				符合	不符合	
1		仅一级要求： 具有自主开发专业检测工具的能力。	该级别服务提供商需具备自主开发专业安全检测工具的能力，如有自主知识产权的工具产品（自主知识产权书、商用产品检测证书、安全产品认证证书等）。			
1	检测阶段	确定检测对象及范围。	确定检测对象及范围的过程记录。			
1		对发生异常的系统进行信息的收集与分析，判断是否真正发生了安全事件。	收集信息的过程及判断依据（过程记录）。			
1		与客户共同确定应急处理方案。	提供应急处理方案（模板及实际项目的应急处理方案）。			
2		应急处理方案应明确检测范围与检测行为规范，其检测范围应仅限于客户已授权的与安全事件相关的数据，对客户的机密性数据信息未经授权不得访问。	应急处理方案的内容中应明确规定检测范围及检测行为规范（模板及实际项目的应急处理方案）。			
2		与客户充分沟通，并预测应急处理方案可能造成的影响。	应急处理方案涉及的风险阐述（风险识别与风险控制措施）。			
2		检测工作应在客户的监督与配合下完成。	应急处理工作流程或其他文档中约定的工作配合/监督机制，相关过程记录。			
2		仅二级/一级要求： 建立有针对常规应用系统、安全设备、常见网络与信息安全	提供相应的检测技术规范列表及各规范内容（范本或应用本），如针对			

序号	要点	条款	需提供证明材料	自评结论		证明材料清单
				符合	不符合	
		事件的检测技术规范。	windows、Aix、Unix、Linux、oracle、Firewalls、Router 等。			
2		仅二级/一级要求：协助客户确定安全事件等级。	信息收集的过程及确定安全事件等级的证明材料。			
2		仅二级/一级要求：应急处理方案应包含对安全事件的抑制、根除和恢复的详细处理步骤。	应急方案应涵盖该内容。			
2		仅二级/一级要求：应急处理方案应包含实施方案失败的应变和回退措施。	应急方案应涵盖该内容。			
2		仅一级要求：建立有完善的检测技术规范及具有对高技术入侵的检测技术能力。	相关技术检测规范，技术人员检测高技术入侵的能力展示。			
2		仅一级要求：具有挖掘系统设备及业务系统安全漏洞的能力。	提供相关漏洞的证明，包括漏洞平台的发布、漏洞库编号等。			
2		仅一级要求：对确认的安全事件启动安全事件管理程序。	提供安全事件管理程序及事件启动条件（安全事件管理程序文件）。			
3		仅一级要求：应急处理方案中应对可能造成的影响进行分析，包括社会影响。	应急处理方案中对社会影响进行分析的证明材料。			
3	抑制阶段	与客户充分沟通，使其了解所面临的首要问题及抑制处理的目的。	沟通的内容及结果。			
3		在采取抑制措施之前，应告知客户可能	应急处理抑制阶段涉及的风险阐述			

序号	要点	条款	需提供证明材料	自评结论		证明材料清单
				符合	不符合	
		存在的风险。	及告知记录。			
3		严格执行抑制处理方案中规定的内容，如有必要更改，须获得客户的授权。	应急抑制处理方案的变更管理（变更管理涉及的文档）。			
3		抑制措施应能够限制受攻击的范围，抑制潜在的或进一步的攻击和破坏行为。	抑制措施的内容。			
3		仅一级要求： 应使用可信的工具进行安全事件的抑制处理，不得使用受害系统已有的不可信文件。	抑制过程中用到的可信工具列表、工具简介。			
3	根除阶段	协助客户检查所有受影响的系统，提出根除的方案建议，并协助客户进行具体实施。	根除建议（方案）的内容。			
3		应明确告知客户所采取的根除措施可能带来的风险。	应急处理根除阶段涉及的风险阐述及告知记录。			
3		找出导致网络或信息安全事件发生的原因，并予以彻底消除。	安全事件得到根除的证明材料。			
3		仅一级要求： 应使用可信的工具进行安全事件的根除处理，不得使用受害系统已有的不可信文件。	根除过程中用到的可信工具列表、工具简介。			
4	恢复阶段	告知客户网络或信息安全事件的恢复方法及可能存在的风险。	应急处理恢复阶段涉及的风险阐述及告知记录。			
4		（如需重建系统时适用该条款） 对于不	重建系统的相关过程记录。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		能彻底恢复配置和彻底清除系统上的恶意文件，或不能肯定系统经过根除处理后是否可恢复正常时，应选择重建系统。				
4		（如需重建系统时适用该条款） 应协助客户按照系统的初始化安全策略恢复系统。	重建系统过程中按照初始化安全策略恢复系统的相关过程记录。			
4		（如需重建系统时适用该条款） 应协助客户验证恢复后的系统是否运行正常，并确认与原有系统配置保持一致。	重建系统过程中关于确认系统配置与原有系统配置是否一致的相关过程记录。			
4		（如需重建系统时适用该条款） 在帮助用户重建系统前需进行全面的数据备份，备份的数据要确保是没有被攻击者改变过的数据。	重建系统过程中关于数据备份的相关过程记录。			
4		（不需重建系统时适用该条款） 应建立重建系统的应急工作流程及规范，并开展重建系统的应急演练工作。	重建系统的应急工作流程及规范，重建系统的应急演练记录。			
4		仅二级/一级要求： 与客户共同制定系统恢复方案，根据实际情况协助客户选择合理的恢复方法。	形成的系统恢复方案及内容。			
4		仅二级/一级要求：（如需重建系统时适用该条款） 帮助客户为重建后的系统建立系统快照。	重建系统过程中关于建立系统快照的相关过程记录。			

序号	要点	条款	需提供证明材料	自评结论		证明材料清单
				符合	不符合	
4		仅一级要求: (如需重建系统时适用该条款) 帮助客户对重建后的系统进行全面的安全加固。	重建系统过程中对系统进行安全加固的相关过程记录。			
4	总结阶段	应保存完整的网络或信息安全事件处理记录, 并对事件处理过程进行总结和分析。	已完成项目的网络安全事件处理过程记录、总结与分析文档。			
5		仅二级/一级要求: 网络与信息安全事件处理记录应具备可追溯性。				
5		提供网络或信息安全事件处理报告。				
5		仅二级/一级要求: 提供详实的网络与信息安全事件处理报告, 完整展现应急处理服务的整个过程。				
5		提供网络或信息安全方面的建议和意见, 必要时指导和协助客户实施。	已完成项目中向客户提供的网络安全建议。			
5		仅一级要求: 对网络与信息安全事件进行总结和分析后, 针对典型案例存入事件知识库。	知识库的案例表。			
5		仅一级要求: 提供关闭安全事件的管理程序。	安全事件的关闭程序(安全事件关闭涉及的文档)。			
5		仅一级要求: 告知客户所发生事件可能涉及到的法律诉讼方面的法律要求或影	应急处理中涉及到司法相关告知的相关文档。			

序号	要点	条款	需提供证明材料	自评估结论		证明材料清单
				符合	不符合	
		响。				
5	上一年度提出的观察项整改情况（如有）					
5						
5						
6	上一年度提出的不符合项整改情况（如有）					
6						
6						

智汇源认证

自评估结论:

经自主评估, 本单位的信息安全应急处理服务满足《信息安全服务 规范》___级要求, 申请第三方审核。

本单位郑重承诺, 本自评估表中所提供全部信息真实可信, 且均可提供相应证明材料。

罗龙 总监

重庆智汇源认证服务有限公司
☎ 139 8308 6348 023-6778 8950
📍 重庆市江北区北滨二路538号7-8-4
🌐 www.cqzhihuiyuan.com

成都智汇源认证服务有限公司
☎ 136 0808 9100 028-8430 1286
📍 成都市高新区天府三街218号1-10-8
🌐 www.sczhihuiyuan.com



质认证

认证范围 : 军工武器产品认证 ; 海陆空产品认证 ; 信息安全资质认证 ; 特种行业资质认证 ; 实验室资质认证 ; 管理体系标准认证 ;

		计量授权			API
武器装备 军标认证	武器装备 保密资格	武器装备 科研许可	武器装备 承制注册	涉密信息 系统集成	航空航天 AS9100
					特种设备