变更记录：

序号	变更原因	变更内容	编制（变更）人/时间	批准人/时间	备注
1	新建	全部，版本A/0	葛方隽/2021.3	吕萍/2021.3	

安全通信网络（S3A3G3）作业指导书					
控制点	安全控制项	备注	测评方法	预期结果或主要证据	符合情况
	a)应保证网络设备的业务处理能力满足业务高峰期需要	为了保证主要网络设备具备足够处理能力，应定期检查设备资源占用情况，确保设备的业务处理能力具备冗余空间。	1)应访谈网络管理员业务高峰时期为何时，核查边界设备和主要网络设备的处理能力是否满足业务高峰期需要，询问采用何种手段对主要网络设备的运行状态进行监控。 一般来说，在业务高峰期主要网络设备的CPU内存最大使用率不宜超过70%，也可以通过综合网管系统查看主要网络设备的CPU、内存的使用情况。 2)应访谈或核查是否因设备处理能力不足而出现过宕机情况，可核查综合网管系统告警日志或设备运行时间等，或者访谈是否因设备处理能力不足而进行设备升级。 查看设备在线时长，如设备在线时间在近期有重启可询问原因。 3)应核查设备在一段时间内的性能峰值，结合设备自身的承载性能，分析是否能够满足业务处理能力。	1)设备CPU和内存使用率峰值不大于70%; 2)未出现宕机情况，网管平台未出现宕机告警日志，设备运行时间较长: 3)业务高峰流量不超过设备处理能力的70%	符合情况：主要网络设备CPU和内存使用率峰值不超过70%，未出现宕机情况，业务高峰期流量不超过设备70%。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：主要网络设备CPU和内存使用率峰值超过70%，业务高峰期流量超过设备承受能力70%。
	b)应保证网络各个部分的带宽满足业务高峰期需要	为了保证业务服务的连续性，应保证网络各个部分的带宽满足业务高峰期需要。如果存在带宽无法满足业务高峰期需要的情况，则需要在主要网络设备上进行带宽配置，保证关键业务应用的带宽需求	1)应访谈管理员高峰时段的流量使用情况，是否部署流量控制设备对关键业务系统的流量带宽进行控制，或在相关设备上启用QoS配置，对网络各个部分进行带宽分配，从而保证业务高峰期业务服务的连续性 2)应该查综合网管系统在业务商峰时段的带宽占用情况，分析是否满足业务需求。如果无法满足业务高蜂期需要，则需要在主要网络设备上进行带宽配置 3)测试验证网络各个部分的带宽是否满足业务高峰期需求	1)在各个关键节点部署流量监控系统，能够监测网络中的实时流量，部署流量控制设备，在关键节点设备品置QoS策略，对关健业务系统的流量带宽进行控制 2)节点设备配置了流量监管和流量整形策略; 3) 各通信链路高峰流量均不大其带宽的70%	符合情况：采取了流量限制措施或各各个关键节点通信线路高峰流量不大其带宽70%。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：各个关键通信线路高峰期流量均大于其带宽70%。

网络架构	c)应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址	根据实际情况和区域安全防护要求，应在主要网络设备上进行VLAN划分。VLAN是一种通过将局域网内的设备逻辑地而不是物理地划分成不同子网从而实现虚拟工作组的新技术。不同VLAN内的报文在传输时是相互隔离的,即一个VLAN内的用户不能和其它VLAN内的用户直接通信，如果不同VLAN要进行通信，则需要通过路由器或三层交换机等三层设备实现	应访谈网络管理员，是否依据部门的工作职能、等级保护对象的重要程度和应用系统的级别等实际情况和区域安全防护要求划分了不同的VLAN,并核查相关网络设备配置信息，验证划分的网络区域是否与划分原则一致。	划分不同的网络区域，按照方便管理和控制的原则为各网络区域分配地址，不同网络区域之间应采取边界防护措施:	符合情况：划分有不同的网络区域并按照方便管理和控制的原则分配网络地址，并采取控制措施。 部分符合情况：无部分符合情况。 不符合情况：未划分不同的网络区域，未根据业务情况划分不同的网络地址，所有都部署在统一网段内，且未采取控制措施。
	d)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段	为了保证等级保护对象的安全，应避免将重要网段部署在网络边界处且直接连接外部等级保护对象，防止来自外部等级保护对象的攻击。同时，应在重要网段和其它网段之间配置安全策略进行访问控制	1)应核查网络拓扑图是否与实际网络运行环境一致 2)应核查重要网络区域是否未部署在网络边界处;网络区域边界处是否部署了安全防护措施 3)应核查重要网络区域与其他网络区域之间，例如应用系统区、数据库系统区等重要网络区域边界是否采取可靠的技术隔离手段，是否部署了网闸、防火墙和设备访问控制列表(ACL)等	1)网络拓扑图与实际网络运行环境一致 2）重要网络区域未部署在网络边界处 3)在重要网络区域与其他网络区域之间部署了网闸、防火墙等安全设备实现了技术隔离	符合情况：网络拓扑与实际运行一致，重要网络区域没有部署在边界，且已经采取措施实现隔离。 部分符合情况：预期结果1,2,3满足一部分为部分符合。 不符合情况：网络拓扑图与实际不一致，重要网络区域部署在边界，且未采取访问控制措施。
	e)应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性	本要求虽然放在“安全通信网络”分类中，实际是要求整个网络架构设计需要冗余。为了避免网络设备或通信线路出现故障时引起系统中断，应采用冗余技术设计网络拓扑结构，以确保在通信线路或设备故障时提供备用方案，有效增强网络的可靠性	应核查系统的出口路由器、核心交换机、安全设备等关键设备是否有硬件冗余和通信线路冗余，保证系统的高可用性	采用HSRP、VRRP 等冗余技术设计网络架构，确保在通信线路或设备故障时网络不中断，有效增强网络的可靠性	符合情况：采用HSRP，VRRP等进行冗余技术设计网络架构，且通信线路采用冗余方式设计。 部分符合情况：部分关键设备未采取冗余方式设计。 不符合情况：所有关键设备均未采取冗余方式设计。

通信传输	a)应采用校验技术或密码技术保证通信过程中数据的完整性	为了防止数据在通信过程中被修改或破坏，应采用校验技术或密码技术保证通信过程中数据的完整性，这些数据包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	1)应核查是否在数据传输过程中使用校验技术或密码技术来保证其完整性 2)应测试验证设备或组件是否保证通信过程中数据的完整性。例如使用File ChecksumIntegrity Verifier、SigCheck 等工具对数据进行完整性校验	1)对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息数据等采用校验技术或密码技术保证通信过程中数据的完整性; 2) File ChecksumIntegrity Verifier 计算数据的散列值，验证数据的完整性	符合情况：在数据传输过程中采取了校验技术或密码技术保证其完整性。 部分符合情况：部分关键数据采用了校验技术或密码技术。 不符合情况：未采取措施在数据传输过程中采取校验技术和密码技术保证其完整性。
	b)应采用密码技术保证通信过程中数据的保密性	根据实际情况和安全防护要求，为了防止信息被窃听，应采取技术手段对通信过程中的敏感信息字段或整个报文加密，可采用对称加密、非对称加密等方式实现数据的保密性	1)应核查是否在通信过程中采取保密措施，具体采用哪些技术措施 2)应测试验证在通信过程中是否对敏感信息字段或整个报文进行加密，可使用Sniffer、Wireshark 等测试工具通过流量镜像等方式抓取网络中的数据,验证数据是否加密	1)对鉴别数据、重要业务数据，重要审计数据、重要配置数据、重要视频数据和重要个人信息数据等采用密码技术保证通信过程中数据的保密性 2)Sniffer. Wireshak可以监视到信息的传送，但是显示的是加密报文	符合情况：在数据传输过程中采取了校验技术或密码技术保证其保密性。 部分符合情况：部分关键数据采用了校验技术或密码技术。 不符合情况：未采取措施在数据传输过程中采取校验技术和密码技术保证其保密性。

可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信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，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心	通信设备可能包括交换机、路由器或其他通信设备等，通过设备的启动过程和运行过程中对预装软件(包括系统引导程序、系统程序、相关应用程序和重要配置参数)的完整性验证或检测，确保对系统引导程序、系统程序、重要配置参数和关键应用程序的篡改行为能被发现，并报警便于后续的处置动作	1)应核查是否基于可信根对设备的系统引导程序、系统程序、重要配置参数和关键应用程序等进行可信验证 2)应核查是否在应用程序的关键执行环节进行动态可信验证 3)应测试验证当检测到设备的可信性受到破坏后是否进行报警 4)应测试验证结果是否以审计记录的形式送至安全管理中心 (2.3)	1)通信设备、交换机、路由器或其他通信设备具有可信根芯片或硬件 2)启动过程基于可信根对系统引导程序、系统程序，重要配置参数和关键应用程序等进行可信验证度量 3)在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心 4)安全管理中心可以接收设备的验证结果记录 (2.3)	符合情况：通信设备例如交换机、路由器均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理中心，并验证。 部分符合情况：预期结果1，2，3，4点满足一部分为部分符合。 不符合情况：未采取措施通信设备例如交换机、路由器均部署了可信芯片或硬件进行可信验证，均基于可信根对引导程序、系统程序，重要配置参数和关键应用程序进行可信验证度量，在检测到可信性破坏后进行报警，并将验证结果送至安全管理