附录 F
安全措施目录

安全措施，附加指导和增强控制

接下来的安全措施目录中提供了一系列关于信息系统安全措施和对策。为了在控制选择和详述过程时使用方便，安全控制以类的方式组织。每个类包含与该类安全功能相关的安全控制措施。一个标准的，双字母的标志符用来唯一地鉴别每个控制类。为了唯一的鉴别每个控制，每个类标志符后都附有一个数字用来指示该控制类内控制的数目。

安全控制框架包括三个主要部分：（1）控制措施；（2）附加指导；（3）增强控制。控制措施中提供了关于对一个信息系统某特定方面所需要的明确安全能力的精确陈述。该控制描述了由组织或信息系统产生的明确的安全相关行为或即将执行的动作。对于控制目录中的某些控制，它提供了一定程度的灵活性来允许组织选择性的定义那些与控制有关联的特定参数的输入值。该灵活性通过控制中的赋值和选择操作来完成。

附加指导中提供了与详细安全控制有关的附加信息。在定义、开发和执行安全目录的时候，希望组织能够恰当的应用附加指导。在某些例子当中，考虑到组织实际的操作环境，人物需求和风险评估，附加指导提供了更多与控制需求或重要因素（以及必须的灵活性）有关的细节描述。另外，对于某些安全控制，应用法则，执行命令、指令、策略、规则、标准和指导文档（例如：OMB文件，FIPS和NISF特殊出版物）都会在附加指导域中列出。

增强控制中提供以下安全能力方面的陈述：（1）为一个基本控制建立附加的，但相关的功能；并/或者（2）增加基本控制的强度。这两种情况中，当一个信息系统由于潜在损失的影响而需要更强的保护，或者当组织基于风险评估的结果要寻求一些对于基础控制的附加功能时，才使用增强控制。增强控制在每个控制中都以顺序的形式编号，因此当增强措施被选择用来补充基本控制时可以很容易被识别。安全控制增加的数字形式的设计只用于鉴别控制框架中的某个特殊的增强措施。该设计既不是增强控制相关长度的指令，也不是增强中的等级关系的假设。

在这份安全控制措施目录中，我们把将会应用于ICS（工业控制系统）的一些措施进行了补充。大部分控制都可以如文中所写的应用于ICS。ICS补充指南与ICS增强补充指南中针对具体的应用环境对所采用的安全控制措施进行了描述。这些控制措施与应用于信息系统中的措施相比，并没有改变。

类： 访问控制 (AC)
CLASS：TECHNICAL

AC-1 访问控制策略和步骤

控制：组织开发、分发和周期性的审查/更新：（i）一个正式的、文档化的访问控制策略提出目的、范围、角色、职责和遵从。（ii）正式、文档化的章程使访问控制策略和相关的访问控制的落实更加容易。

附加指导： 访问控制策略和章程跟可用的联邦法律、指示、政策、规章、标准和指南一致。访问控制策略能作为组织的通用信息安全策略的一部分包被含。针对通常的安全项目和当需要访问控制章程的特定的信息系统，开发访问控制章程。NIST SP800-12在安全策略和章程方面提供了指南。

增强控制： 无。

LOW AC-1	MOD AC-1	HIGH AC-1

AC-2 帐户管理

控制：组织管理信息系统帐户，包括建立、激活和修改、审核、失效和删除帐户。组织审核信息系统帐户 [指定：组织定义的时间周期]。

附加指导：帐户管理包括帐户类型的鉴别（也就是个人、组、系统），组成员条件的确定和相关授权的分配。组织识别信息系统的授权用户和特定的访问控制权利/特权。组织基于如下允许访问信息系统：（i）一个有根据的需要知道的是由指定的官方职责和满足所有的人员安全标准（ii）有计划的系统用途。针对建立信息系统帐户的需求和为满足这些需求，组织要求适当的鉴别。组织明确地授权和监督客人/匿名帐户的使用，删除、使失效或者是使不必要的帐户安全。当终止、转移信息系统使用者，或删除、使相关的帐户失效或使相关的帐户安全，组织要确保帐户管理者被通知。当信息系统使用或者须知发生改变时，也要通知账户管理人。

ICS附加指导：账户管理可以包括多种账户类型（基于角色的，基于设备的，基于属性的）。单位应删除，禁用或对缺省账户提供安全维护。缺省的密码需要修改。如果预先定义了对工作站，硬件，或者现场设备的接入优先权，单位应根据组织风险评估来实施物理安全策略和章程。在某些情况下，组织认为实施措施或者措施加固是不合适或者不可取的（例如对远程终端，仪表，继电器），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制

(1) 组织使利用自动的机制来支持对信息系统帐户的管理。

ICS增强附加指导：对于某些ICS部件（如，现场设备），账户管理的自动机制不可

用，应采用手动。

(2) 信息系统自动地终止临时的和非常时期的帐户在[指定：对每一类帐户组织定义的时间周期之后。

(3) 信息系统自动地停止非活动的帐户在[指定：组织定义的时间周期]之后。

(4) 组织利用自动的机制来确保帐户的创建、修改、使失效和终止活动被审计，并且在需要的时候，通知适当的人。

LOW AC-2	**MOD AC-2 (1) (2) (3) (4)**	**HIGH AC-2 (1) (2) (3) (4)**

AC-3 强制访问控制（ACCESS ENFORCEMENT ）

控制：信息系统根据应用策略执行指定的系统访问控制授权。

附加指导：组织采用访问控制策略（如：基于身份的策略，基于角色的策略，基于规则的策略）和相关的访问执行机制（如：访问控制列表，访问控制许可，密码学）实现信息系统中的用户（或者用户进程）与对象（包括设备，文件，纪律，进程，程序，域）间的访问控制。为了给系统提供更好的信息安全，除了在信息系统层面实现访问控制外，还要在必要时在应用层实现强制访问机制。如果采用对储存信息加密作为强制访问机制，应使用与FIPS 140-2一致的密码学算法。

ICS附加指导：强制访问控制机制绝对不可以对ICS的正常运行产生负面影响。NIST SP 800-82中提供了ICS访问控制指南。

NIST SP 800-82 ICS特别推荐与指南：ICS可以采用的一般的访问控制方式包括：基于角色的访问控制，Web服务器，VLAN，拨号和无线等。

（1） 在ICS中使用基于角色的访问控制的优点是可以减少设备维护个人访问控制权限的负担。

（2） 一般的ICS产品上都集成了Web服务器的功能，这样可以使得远程配置更容易，但同时也带来了风险。

（3） 在很多的ICS网络中都使用了VLAN，它可以限制不必要的流量泛洪。

（4） 拨号调制解调器在ICS网络中使用的也很多，主要用于当远程终端设备发生故障时的技术支持请求，拨号软件和设备应满足如下条件：具有回叫能力，可以存储来电者的信息；“猫”要有使用密码；可以识别不同位置的“猫”；远程访问软件的用户名和口令要唯一；“猫”在不用时要拔掉。

（5） 在ICS网络中采用无线访问方式是基于风险的决定，使用无线设备存在如下要求：安装天线时要实地考察，避免攻击者可以利用地形使用定向天线；无线访问要具有EAP等认证功能；无线接入点和数据服务器要在和ICS网络相连但是不同的网络中；无线接入点要有SSID；无线设备应是Windows域中不同的

单元；通信要具备加密和完整性保护。

增强控制:

(1) 信息系统保证只有授权人（安全管理员）可以访问（在硬件、软件或者部件上配置的）安全功能和信息。

增强附加指导：明确的授权人包括：安全管理员，系统与网络管理员，其他特许用户。特许用户指那些对系统控制，监视和管理功能有访问权利的人，比如：系统管理员，信息系统安全官员，维护者，系统程序员。

ICS增强附加指导：特权用户对专有功能的访问也应该根据设备（远程终端和现场设备）来限制。

ICS增强控制:

(2) 根据被认可的组织程序，ICS对将影响设备，人员和环境安全性的专有功能要求双重授权。

ICS增强附加指导：当为了保障人员和环境安全需要采取紧急相应时（例如安全阀），组织可以不采用双重批准机制。

LOW AC-3	MOD AC-3 (1)	HIGH AC-3 (1)

AC-4 信息流强制访问控制（INFORMATION FLOW ENFORCEMENT）

控制：信息系统根据应用策略执行指定的系统中和互联系统间的信息流授权。

附加指导：信息流控制只针对信息系统中和信息系统间的信息流动，而不考虑之后对这些信息的访问。流控制的例子包括：禁止控制信息以明文方式进入互联网，屏蔽声称来自组织内部的外部流量，只传递由内部网络代理发往互联网的网络请求。组织采用信息流控制策略和执行机制来控制信息系统内部和互连的网络间的指定源与目标（如：网络，个人，设备）间的信息流。流控基于信息和信息路径的特征。强制流控的具体实例可以在边界保护设备上找到，这些设备使用规则或建立配置项来限制信息系统服务或者实现包过滤功能。相关的安全控制：SC-7。

增强控制:

(1) 信息系统采用外部信息、源和目的对象列表作为流控基础来实施强制信息流控制。

增强附加指导：强制信息流控制采用外部列表控制某种类型的信息流。

(2) 信息系统采用受保护的处理域（域类型强制）作为流控决定的基础。

(3) 信息系统采用动态安全策略机制作为流控决定的基础。

LOW Not Selected	MOD AC-4	HIGH AC-4

AC-5 职责分开

控制：信息系统通过分配存取授权来实施职责分离

附加指导：组织根据需要建立适当的职责分离来消除在个人职责方面的利益冲突。存在信息系统方面的访问控制软件来防止用户有所有可能的授权或对信息进行访问而在没有同谋的情况下可以进行欺骗性的行为。职责分离的例子包括：(i) 任务功能和截然不同的信息系统支持功能应在不同的人/角色之间分开(ii) 不同的人完成信息系统支持功能(例如系统管理，系统变成，质量保证/测试，配置管理和网络安全)；和(iii) 管理访问控制功能的安全人员不能赋予审计功能。

ICS附加指导：在某些情况下，组织认为实施责任分离是不合适或者不可取的（例如组织只有一个人来执行所有的角色或者ICS并不区分角色），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：无。

LOW Not Selected	MOD AC-5	HIGH AC-5

AC-6 最小特权

控制：信息系统针对特定任务的执行实施最受限制的权利/特权或用户所需要的访问控制（或代表用户的进程）。

附加指导：组织针对特定的职责和信息系统（包括特定的端口、协议和服务），利用最小特权的概念，依照必要的风险评估来充分地降低组织的运行、组织的资产和个人的风险。

ICS附加指导：在某些情况下，组织认为实施最小特权是不合适或者不可取的（例如组织只有一个人来执行所有的角色或者ICS并不区分角色），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：无。

LOW Not Selected	MOD AC-6	HIGH AC-6

AC-7 失败的登陆尝试

控制：当一个用户在一个[指定：组织定义的时间段] 连续无效的企图访问，信息系统执行 [指定：组织定义的数]的的限制。信息系统自动地[选择：锁定帐户/节点直

到由管理员解锁，锁定帐户/节点针对[指定：组织定义的时间段]，根据[指定：组织定义的延迟算法]到下一次登陆提示的延迟]当超过不成功登陆尝试的最大值时。

附加指导：为了防止DoS攻击，信息系统自动执行锁定。但是这种锁定往往是暂时的，在系统规定的一段时间之后自动释放。

ICS附加指导：在某些情况下，组织认为实施自动锁定是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。例如，根据风险评估，账户或者节点不能锁定，那么当连续非法登陆次数超过组织规定的门限值时，ICS记录所有不成功的登陆企图，并向ICS安全人员发出警告。

增强控制：

(1) 当登陆尝试次数超过系统规定最大值时，信息系统自动锁定帐户/节点，直到管理员来解锁。

LOW AC-7	MOD AC-7	HIGH AC-7

AC-8 系统使用提示

控制：信息系统显示经过批准的、校准过的通告信息，在允许系统访问通知有影响力的用户之前； (i)可以监控、记录系统使用，并且可审计；(iii)禁止未授权的使用系统，否则接受刑事和民事惩罚；(iv)使用系统表明同意监控和记录。通告信息提供了适当的秘密和安全通知（基于相关的保密和安全策略），并保持在屏幕上，直到用户采取了明确的行动来登陆信息系统。

附加指导：保密与安全策略与法规，执行规定，命令，策略，规则，标准和指南相一致。当有用户登录信息系统时，系统的通知消息可以警告条的形式呈现出来。对公共的可访问系统： (i)在授权访问之前，相对于显示信息，系统使用信息是可用的；(ii) 这里不涉及监控、记录或审计，因为这些系统的秘密的装置通常禁止那些活动；(iii) 通知公共用户系统信息，包括系统授权使用描述。

ICS附加指导：在某些情况下，组织认为实施系统使用通知是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。例如，物理通知可以张贴在ICS机构中。相关的安全措施：PL-2。

控制加强：无。

LOW AC-8	MOD AC-8	HIGH AC-8

AC-9 以前登陆提示

控制：信息系统提示用户，成功登陆、上次登陆的时间，上次登陆的地点、自上次成功登陆后不成功登陆的次数。

附加指导：无。

控制加强：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

AC-10 并发会话控制

控制：信息系统限制任何用户并发会话数为[指定：组织定义的会话数]。

附加指导：无。

ICS附加指导：一些ICS或者组件可能不允许并行会话受到限制。在某些情况下，组织认为实施并行会话控制是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。例如，物理通知可以张贴在ICS机构中。相关的安全措施：PL-2。

控制加强：无。

LOW Not Selected	MOD Not Selected	HIGH AC-10

AC-11 会话锁定

控制：在组织定义的一个特定的静止时期后，信息系统通过发起一个会话锁定来保持有效来防止对系统的进一步的访问，直到用户使用合适的标识和鉴别程序来重新建立访问。

附加指导：用户能直接发起会话锁定机制。在组织定义的一个特定的静止时期后，信息系统也自动地激活会话锁定机制。会话锁定不是退出信息系统的替代品。组织定义的静止时期要符合联邦政策，例如，与OMB 06-16 备忘录相一致。对于远程访问和移动设备，组织定义的静止时间应不超过30分钟。

ICS附加指导：ICS可能使用会话锁定来阻止对指定工作站/节点的访问。对于ICS中指定的工作站和节点，在组织规定的一段时间之后，ICS自动启动会话锁定机制。在某些情况下，不推荐采用ICS操作者工作站/节点会话锁定。在某些情况下，组织认为实施会话锁定是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。例如，对ICS操作者工作站/节点的访问可以通过严格的物理安全措施来限制。会话锁定并不可以取代ICS的系统退出。NIST SP 800-82中提供了ICS中使用会话锁定的指南。（NIST SP 800-82附录E里面提到了会话锁定的问题，和以上表述类似）相关的安全措施：PL-2。

控制加强：无。

LOW Not Selected	MOD AC-11	HIGH AC-11

AC-12 会话终止

控制：信息系统自动地终止会话在[指定：组织定义的时间段]静止之后。

附加指导：当有用户（或信息系统）企图通过外部非组织控制网络（如：互联网）访问组织信息系统时，开启远程会话。

ICS附加指导：一些ICS或者组件不可以或者不允许中断会话。在某些情况下，组织认为实施会话终断是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制

(1) 将自动会话终止应用于本地和远程会话。

LOW Not Selected	MOD AC-12	HIGH AC-12 (1)

AC-13 监督与审核－访问控制

控制：组织监督和审核用户关于信息系统访问控制的执行和使用的行为。

附加指导：依照组织的流程，针对对不恰当的行为，组织审核审计记录（例如用户行为日志）。组织调查任何与系统相关的行为的不寻常的信息，并周期性地审核对授权的修改。组织更频繁地审核担当重要信息系统角色和职责用户的行为。审计记录审核的范围是以FIPS 199的信息系统影响等级为根据的。例如，对于低影响系统，只需要对网络代理或者email服务器之类的中心点进行频繁的安全日志审核，或者在有特殊授权的条件下，对某些审计记录进行审核，不然没必要对所有的工作站都进行频繁的安全日志审核。NIST SP 800-92 中提供了关于计算机安全日志管理的相关指南。

ICS附加指导：一些ICS不支持自动机制。在某些情况下，组织认为实施自动监管和用户行为复审是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

控制加强：

(1) 组织利用自动机制来是审核用户的行为更加方便。

LOW AC-13	MOD AC-13 (1)	HIGH AC-13 (1)

AC-14 无标识与认证的操作许可

控制：组织识别并记录在信息系统上执行没有标识或认证的特定的用户行为。

附加指导：组织允许对公共的WEB站点或其他公共的可用的信息系统的没有标识和鉴别的有限的用户活动（例如，从*http://www.firstgov.gov*访问联邦信息系统）。相关的安全控制：IA-2。

控制加强：

(1) 组织允许没有标识和鉴别的的行为，只在完成任务目标所必须的的范围内。

LOW AC-14	MOD AC-14 (1)	HIGH AC-14 (1)

AC-15 自动标识

控制：信息系统使用标准命名惯例标记输出，来识别任何特定的分发、处理或分发指示。

附加指导：自动标识指在外部介质（如信息系统的硬件文档输出）上进行标记。这种外部标记与AC-16中的内部数据结构标签不同。

ICS附加指导：一些ICS不支持自动标记（外部标记）。在某些情况下，组织认为实施自动标记是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

控制加强：无。

LOW Not Selected	MOD Not Selected	HIGH AC-15

AC-16 自动标签

控制：信息系统在存储、处理和传输中进行适当的标识信息。

附加指导：自动标签指在信息系统内部，对内部数据结构（如：记录，文件）进行标签。如下情况下需要进行自动标签：(i) 访问控制需要；(ii) 根据特定的分发、处理或分发指令；和(iii) 信息系统安全策略的需要。

ICS附加指导：一些ICS不支持自动标记（内部标记）。在某些情况下，组织认为实施自动标记是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

控制加强：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

AC-17 远程访问

控制：组织授权、监督和控制所有对信息系统的远程访问。

附加指导：远程访问是指用户（或信息系统）通过外部非组织控制网络（如：互联网）对组织信息系统进行访问。远程访问包括拨号、宽带和无线。远程访问控制只应用于信息系统，不用于公共的WEB服务器或针对公共访问设计的特定系统。组织通过拨号连接限制访问（例如基于请求源限制访问）或防止遭受未授权的连接或授权连接的破坏（例如使用虚拟私有网络技术）。NIST SP 800-63 中提供了远程电力认证方面的指南。如果采用基于令牌的加密访问控制，并且将联邦PIV指南证书作为身份令牌，那么这种访问控制系统就与FIPS201和NIST SP 800-73和800-78相一致了。NIST SP 800-77中提供了关于基于IPsec的VPN技术相关的指南。相关的安全控制为：IA-2。

ICS附加指导：只有在必要的情况下，并且已经得到了批准和认证，才可以使用ICS部件（控制中心，现场）的远端访问。组织应考虑ICS远程用户访问的多因素认证。NIST SP 800-82 中提供了ICS远程访问的指南。

NIST SP 800-82 ICS特别推荐与指南：远程访问采用加密的协议，并且采用多因素认证。可以通过企业网内的系统与控制网络进行通信，但是要在控制网络防火墙上实现双因素认证。

控制加强：

(1) 组织利用自动机制来是监督和控制远程访问方式更加容易。

ICS增强附加指导：一些ICS不支持远端访问控制。如果有特殊情况，组织认为实施自动标记是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

(2) 组织利用加密来保护远程访问会话的机密性。

ICS增强附加指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。如果有特殊情况，组织认为使用密码学是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

(3) 组织通过一些可管理的访问控制点来控制所有的远程访问。

(4) 组织只对强制操作需求提供特许功能的远程访问，并在信息系统的安全计划中

将这种访问的原因记录下来。

LOW AC-17	**MOD AC-17 (1) (2) (3) (4)**	**HIGH AC-17 (1) (2) (3) (4)**

AC-18 限制无线访问

控制：对于无线网络，（i）组织应当建立使用限制和实现指导准则；（ii）授权、监视和控制无线网络对信息系统的访问。由组织中适当的官员来批准无线网络技术的应用。

附加指导：NIST SP 800-48和800-97中提供对无线网络安全的指导。NIST SP 800-94中提供了无线侵入检测与阻止的相关指南。

ICS附加指导：无线技术包括，但不局限于微波，卫星，分组通信（UHF/VHF），802.11x和蓝牙。

增强控制：

(1) 组织应采取认证与加密技术来保护通过无线网络对信息系统的访问。组织利用加密来保护远程访问会话的机密性。

ICS增强附加指导：ICS总是分别支持可用性，完整性和加密性。因此，在无线访问中使用密码学应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。在某些情况下，组织认为使用密码学是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

(2) 组织扫描未授权的无线接入点并在发现后采取适当措施。

增强附加指导：组织在重要的信息系统等设备中对未授权的无线接入点进行全面扫描。扫描并不局限于重要的信息系统。

LOW AC-18	**MOD AC-18 (1)**	**HIGH AC-18 (1) (2)**

AC-19 便携与移动设备访问控制

控制：组织（i）建立便携和移动设备的使用限制和实施指南；（ii）授权、监视和控制对信息系统的设备访问。

附加指导：使用便携和无线设备（比如：笔记本，个人数字设备，移动电话和其他具有网络连接能力，物理位置可周期性变更的计算和通信设备）访问组织信息系统要遵守组织安全策略和章程。安全策略和章程包括设备识别和认证，防护软件（恶

意代码检测，防火墙）的强制安装，配置管理，恶意代码扫描设备，杀毒软件升级，主要软件的升级和补丁扫描，执行操作系统（或其他辅助软件）完整性扫描，拆除没必要的硬件（如：无线设备，红外设备）。对便携和移动设备中的信息保护（如采用密码学机制为存储或控制域外传输的信息提供加密和完整性保护）属于媒体保护子类。相关的安全控制：MP-4，MP-5。

ICS附加指导：组织应考虑关闭不用的或不必要的I/O端口。

增强控制：无。

LOW Not Selected	MOD AC-19	HIGH AC-19

AC-20 使用外部信息系统（USE OF EXTERNAL INFORMATION SYSTEMS）

控制：组织为授权用户建立如下条款和条件（i）从外部信息系统访问信息系统；（ii）使用外部信息系统处理、存贮和（/或）传输受控信息。

附加指导：外部信息系统是指这样一些信息系统或部件，他们位于组织建立的安全边界外，组织不能直接控制他们的安全措施的采用和安全措施有效性评估。外部息系系统包括但不局限于个人信息系统（如，计算机，移动电话或者个人数字辅助设备）；商业或公共场所（如：旅馆，会务中心或机场）中的私有计算通信设备；非联邦政府所有或控制的信息系统；不属于组织，不被组织所使用或组织不直接控制的联邦信息系统。

授权个人包括组织内人员，承包人，任何被授权访问组织信息系统的人。和（/或）传输受控信息。这条措施不可应用于采用外部信息系统访问组织信息系统和用于公共访问的信息（如：个人通过公共接口进入组织信息系统访问联邦数据）。组织所建立的使用外部信息系统的条款和条件应与组织安全策略和章程相一致。条款中至少包括：（i）从外部信息系统可以访问的组织信息系统中的应用类型；（ii）外部信息系统可以处理、存贮和（/或）传输的最大FIPS 199信息安全等级。

增强控制：只有在如下情况下，组织才允许有权限的个体使用外部信息系统访问信息系统或处理、存贮或者传输组织的受控信息：（i）组织能够验证外部系统中作采用的安全措施就是组织信息安全策略和系统安全计划中所指定的；或（ii）组织批准了信息系统连接或与外部信息系统的主管实体达成了处理一致。

LOW AC-20	MOD AC-20 (1)	HIGH AC-20 (1)

类： 安全意识和培训 (AT)
CLASS：OPERATIONAL

AT-1 安全意识和培训的策略与步骤

控制：组织开发、分发和周期性的审核/更新：(i)一个正式的、文档化的安全意识和培训策略提出目的、范围、角色、职责、管理委托、组织实体间协调和遵从；和(ii)正式的文档化的流程使安全意识和培训策略和相关的安全意识和培训控制的落实更容易。

附加指导：安全意识、培训策略和流程和可用的联邦法律、指示、政策、规章、标准和指南一致。安全意识和培训策略能作为组织通用信息安全策略的一部分被包含。针对通过用的安全项目（program）和特定的信息系统，当需要时，能开发安全意识和培训流程。NIST SP800-16和800-50在安全意识和培训方面提供指南。NIST SP-800-12在安全策略和流程上提供指南。

控制加强：无。

LOW AT-1	MOD AT-1	HIGH AT-1

AT-2 安全意识

控制：当系统发生改变时，或之后[指定：组织指定频率，至少一年]，在组织授予信息系统用户（包括经理和高级管理者）访问权力之前，组织应为用户提供基本的安全常识培训。

附加指导：感觉组织和授权访问的信息系统的具体需求，组织决定安全常识培训的合适内容，组织的安全意识与5 C.F.R 930.301中板块C中的要求和NIST SP 800-50中的指南相一致。

ICS附加指导：安全意识包括对策略，标准实施程序，安全趋势和脆弱性的最初审查与阶段性复审。ICS安全意识程序应与组织建立的安全意识策略相一致。

控制加强：无。

LOW AT-2	MOD AT-2	HIGH AT-2

AT-3 安全培训

控制：组织识别出在系统开发生命周期中具有重要的信息系统安全角色和责任的人，并将这些角色和责任记录下来，并在(i)授权访问系统或执行指定指责之前或(ii)系统发生改变时，提供适当的信息系统安全培训，其后[指定：组织定义的时间周期]。

附加指导：组织根据组织和员工授权访问的信息系统的特定需求，确定适当的安全

培训内容。除此之外，组织保证系统管理者，系统经理和其他可以访问系统层软件的人员都经过了与各自职责相关的适当的技术培训。组织的安全培训计划与5 C.F.R 930.301中板块C中的要求和NIST SP 800-50中的指南相一致。

ICS附加指导：安全培训包括对策略，标准实施程序，安全趋势和脆弱性的最初审查与阶段性复审。ICS安全培训程序应与组织建立的安全意识策略相一致。

控制加强：无。

LOW AT-3	MOD AT-3	HIGH AT-3

AT-4 安全培训记录

控制：组织记录和监督单个信息系统安全培训活动，包括基本的安全意识培训和特定的信息系统安全培训。

附加指导：无。

控制加强：无。

LOW AT-4	MOD AT-4	HIGH AT-4

AT-5 与安全组织和联盟的联系

控制：组织应与特殊的利益组织、专业的论坛、专业的联盟、新工作组和与组织相似的安全专家组建立和保持联系，以保证拥有最新的安全实践、安全技术和其他诸如威胁、脆弱性和事故之类的安全相关信息。

附加指导：为了在技术快速更新和威胁不断变化的环境中，为组织中的人员提供持续的安全教育和培训，组织应与安全领域内的指定组织和联盟建立长远的联系。应根据组织的任务需求选择建立联系的组织和联盟。信息系统的威胁、脆弱性和事故等信息共享行为应与可用的联邦法律、指示、政策、规章、标准和指南一致。

控制加强：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

类： 审计与责任 (AU)
CLASS：TECHNICAL

AU-1 审计和责任追究策略及过程

控制：组织结构开发、发布及周期性回顾/更新以下内容：(i)正式的，形成文件的，阐释目的、范围、角色、责任及顺应性的审计和责任追究策略；(ii)可以推进审计，责任追究策略及相关的审计和责任追究控制的正式的文件形成流程。

附加指导：审计和责任追究策略及流程符合联邦法律、命令、政策、规范、标准和指导性原则的精神。审计和责任追究策略可能属于组织的总体信息安全策略的一部分。审计和责任追究策略可能因为总体的安全计划和需要的特定信息系统而被拓展。NIST Special Publication 800-12对处理安全政策和流程提供了指导性意见。

控制加强：无。

LOW AU-1	MOD AU-1	HIGH AU-1

AU-2 审计事件

控制：信息系统产生对如下事件的审计记录：[赋值： 组织定义的审计事件].

附加指导：该措施的目的是为了记录那些与信息系统安全相关的重要的审计事件。组织指明哪些信息系统部件执行审计行为。审计行为能够影响信息系统的效率。所以，组织基于风险评估确定哪一个事件需要在一个通常的基础上进行审计，并且确定哪一个事件需要相应于特殊环境的审计。审计记录可以在很多层面上产生，比如在信息穿越网络的包层面上产生。为审计记录的提取选择一个合适的层面是审计能力中重要的一项，它可以使指明问题的根本原因更容易。除此之外，通过选择每个系统记录的信息，可以加强安全审计功能与网络健康和状态监视功能的相互支持。*http：//csrc.nist.gov/pcig/cig.html*的检查列表和配置指导性文件提供了审计事件的推荐列表。组织定义了足以去提供安全事件的事后调查的审计事件。NIST SP 800-92种提供了关于计算机安全日志管理的相关指南。

ICS附加指导：大部分ICS都在应用层完成审计。一些ICS可能没有这个特性。在某些情况下，组织认为实施审计事件是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。

控制加强：

(1) 信息系统提供了编辑审计记录的能力，这些记录来自多重部件，这些部件遍布于系统的逻辑层面、物理层面及相关于时序的审计痕迹中。

(2) 信息系统提供对审计事件选择的集中管理的能力，事件选择被单独的系统部件所审计。

(3) 组织对组织定义的审计事件进行周期性的审核和升级。

LOW AU-2	MOD AU-2 (3)	HIGH AU-2 (1) (2) (3)

AU-3 审计记录的内容

控制：信息系统捕捉审计记录中的足够的信息，以便建立什么事件发生了、事件的来源、事件的结果的记录。

附加指导：对大多数审计记录而言，审计记录内容包括：(i) 事件的日期和时间；(ii) 发生事件的信息系统部件 (如：软件，硬件)； (iii) 事件类型；(iv)用户/对象ID；(v) 事件的结果(成功或者失败)。NIST SP 800-92中提供了关于计算机安全日志管理的指南。

增强控制：

(1) 信息系统能够在审计报告中提供附加的、更详细的信息，这些信息是关于审计事件的类型、位置、主题的。

(2) 信息系统可以提供对审计记录中的内容的集中管理，这些内容是由遍布整个系统的单独的部件提供的。

LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)

AU-4 审计存储容量

控制：组织结构分配足够的审计记录存储空间，以便减少空间被“撑爆”的可能性。

附加指导：考虑到将要进行的审计和在线审计处理要求，组织提供足够的审计记录存储空间。相关的安全措施：AU-2，AU-5，AU-6，AU-7，SI-4。

增强控制：无。

LOW AU-4	MOD AU-4	HIGH AU-4

AU-5 审计处理失败响应

控制：当面临审计失败或者审计存储空间达到极限的情况，信息系统会向相关的组织负责人员发出警报并且采取如下的附加措施：[Assignment： 组织预先确定的应急措施 (例如：关闭信息系统，覆盖最旧的审计记录，停止产生审计记录)].

附加指导：审计处理失败包括：软硬件错误，审计获取机制失败，审计存储空间达到/超出极限。相关的安全措施：AU-4。

ICS附加指导：一般来说，审计记录处理并不在ICS上执行。在某些情况下，组织认为实施审计监视是不合适或者不可取的(或者产生负面影响，影响安全性，可靠性)，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：

(1) 当分配的审计记录存储空间达到[指定：组织所定义的最大审计记录存储能力]时，信息系统发出警告。

(2) 当发生下列审计失败事件时，信息系统发出实时警告。[指定：组织定义的需要实时警告的审计失败事件。]

LOW AU-5	MOD AU-5	HIGH AU-5 (1) (2)

AU-6 审计监控、分析及报告

控制：组织结构定期的回顾/分析审计记录，这些记录是记录不恰当的/不寻常的行为、调查到的可疑行为或者侵犯行为，并向相关人员报告这些事件，和采取必要的措施。

附加指导：无。

增强控制：

(1) 组织采用自动的机制将审计监控、分析、报告联结成一个完整的审计过程。

(2) 组织采用自动机制，对如下存在安全隐患的不安全或者异常行为向安全人员发出警告：[指定：组织定义的需要警告的不安全或异常行为列表。]

LOW Not Selected	MOD AU-6 (2)	HIGH AU-6 (1) (2)

AU-7 审计缩减和产生报告

控制：信息系统提供一个审计归约和报告产生功能。

附加指导：审计归约、回顾、报告工具支持事后对于安全事件进行不改变原审计记录的调查。

ICS附加指导：一般来说，审计处理和生成报告并不在ICS上执行。在某些情况下，组织认为实施审计处理和生成报告是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：

(1) 信息系统提供自动处理审计记录的功能，这些记录是基于可以设定的事件标准选择出来的。

LOW Not Selected	MOD AU-7 (1)	HIGH AU-7 (1)

AU-8 时间戳

控制：信息系统在审计记录产生时使用时间戳。

附加指导：审计记录的时间戳（包括日期和时间）是由内部信息系统的计时装置产生的。

增强控制：

(1) 组织同步内部信息系统时钟[指定：组织定义的频率]。

LOW AU-8	MOD AU-8 (1)	HIGH AU-8 (1)

AU-9 审计信息保护

控制：信息系统保护审计信息和审计工具，使之避免受未授权访问、修改和删除行为的破坏。

附加指导：审计信息包括审计信息系统行为成功的所有信息（如：审计记录，审计设置，审计报告）。

增强控制：

(1) 信息系统在hardware-enforced, write-once media上产生审计信息。

LOW AU-9	MOD AU-9	HIGH AU-9

AU-10 不可否认性

控制：信息系统有能力去确定是否一个既定的个体进行了一个特定的行为。

附加指导：个体特殊行为包括产生信息、发送信息、认可信息（例如：标明并发或者签署一个合同）或者得到一个消息。不可否认性保护用来免除事后来自一个没有进行某项操作的个体的“无根据请求”。不可否认性保护个体免遭过后来自一个没有创作某个文件的作者、一个没有传送某个消息的发送者、一个没有得到某个消息的接收者、或者一个已经签过名的签名者的诉讼请求。不可否认性保护能够用于确定是否信息来自一个个体或者是否一个个体采取了特殊行为 (特殊行为包括：发一封电邮、签署合同、批准请求)或者获得特殊的信息。不可否认型可以通过采用多种技术或机制（如，数字签名，数字消息收据，时间标签）实现。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

AU-11 审计存储

控制：为方便安全事故提供事后调查和满足组织信息保留要求和规定，组织在[指定：组织定义的时间间隔]内，保留设计记录。

附加指导：组织保留审计记录直到这些记录不会再被行政，法律，审计或者其他操作目的所使用。例如，保留与FOIA请求，传票或者法律强制行为相关的审计记录。与此类行为相关的审计记录标准分类和标准响应过程已经得到了制定和传播。NIST SP 800-61中提供了计算机安全事故处理和审计记录保留的相关指南。

增强控制：无。

LOW AU-11	MOD AU-11	HIGH AU-11

类： 认证、认可与安全评估(CA)
CLASS：MANAGEMENT

CA-1 证书、认可、安全评估政策和流程

控制：组织结构开发、发布及周期性回顾/更新以下内容：(i)正式的、形成文件的、阐释目的、范围、角色、责任及顺应性的安全评估和证书及授权策略；(ii)推动安全评估和证书以及授权政策和相关的评估、证书、及授权控制的正式的文件形成流程。

附加指导：安全评估、证书、授权策略及流程符合联邦法律、命令、政策、规范、标准和指导性原则的精神。安全评估、证书、授权策略可能属于组织的总体信息安全政策的一部分。安全评估、证书、授权策略可能因为总体的安全计划和必须的特定信息系统而被拓展。组织定义什么是信息系统的重要改变以保持一致的安全重认证。NIST Special Publication 800-53A对安全控制评估提供了指导性意见。NIST Special Publication 800-37对处理安全证书和授权提供了指导性意见。NIST Special Publication 800-12对于安全政策和流程提供了指导性意见。

增强控制：无。

LOW CA-1	MOD CA-1	HIGH CA-1

CA-2 安全评估

控制：组织在信息系统中处理了一个安全控制评估[任务：定义组织结构的时间周期，至少一年一次]，以便确定恰当的实施控制、合乎要求的运行、产生相关于满足系统安全需要的实施程度。

附加指导：该措施是为了满足FISMA的要求：应根据风险对主要的信息系统中的每一个系统的管理、操作和技术措施进行评估，至少每年一次。FISMA的每年一次安全措施评估的要求不应被组织理解为是要在原有安全验证和授权过程中已经存在的需求的基础上再增加评估要求。为了满足FISMA每年一次的评估要求，组织可以利用通过下面这些渠道获取安全措施评估结果，包括但不局限于：(i) 信息系统授权与重授权中的安全认证（见CA-4）；(ii) 持续监督(见 CA-7)；(iii) 正在进行的系统开发生存中的信息系统测试与评估 (假设测试与评估结果是通用的，而且与安全措施有效性判断相关). 可以采用依然有效的当前安全评估结果，也可以根据需要补充新的评估。评估信息的重用对于获取一个能够产生决定信息系统实际安全状态的广泛的、低成本的和完整的安全项目至关重要。

OMB并不要求对组织信息系统中所有的安全措施每年都进行一次评估。依据OMB策略，组织必须每年根据以下原则对安全措施中的一部分进行评估：(i) FIPS 199 信息系统安全等级；(ii) 组织为了保护信息系统选择和采用的具体的安全措施；(iii) 依据信任等级来决定安全措施的有效性。组织应在三年的认证周期内对所有的安全措施进行评估。组织可以用当年的安全认证中的评估结果来满足FISMA的评估要求（见CA-4）。NIST SP 800-53A 中提供了关于重用当前评估结果的安全措施评估的指南。

相关的安全措施：CA-4，CA-6，CA-7，SA-11。

ICS附加指导：组织保证评估不影响ICS的功能。评估者充分理解公司的信息与ICS安全策略、步骤和与特别的设备与程序相关的具体的健康，安全和环境风险。在评估开始之前，ICS产品可能需要离线，并且复制到可行的设备（盘区）。假如ICS必须离线评估，可以将评估安排在任何可能的计划好的ICS停机阶段。在某些情况下，组织认为实施ICS在线测试是不合适或者不可取的(或者产生负面影响,影响安全性，可靠性），组织应记录下使用复制系统的原因。

增强控制：无。

LOW CA-2	MOD CA-2	HIGH CA-2

CA-3 信息系统连接

控制：组织使用系统连写协议授权所有的来自信息系统的、到达安全边界外的其他信息系统的连接，并持续监控/控制这些系统连接。

附加指导：由于FIPS 199安全等级之应用于单个信息系统，组织必须仔细考虑当系统与其他具有不同的安全需求和安全措施信息系统相连时所引入的风险，无论这种系统是在组织内部还是外部。风险考虑同时也包括同一个网络中的信息系统。NIST SP 800-47为连接信息系统提供了指南。相关的安全措施：SC-7，SA-9。

增强控制：无。

LOW CA-3	MOD CA-3	HIGH CA-3

CA-4 安全认证

控制：组织处理了一个安全控制评估，此评估在信息系统内部、目的在于确定实现恰当的控制、合乎要求的运行、产生相关于系统安全需要的程度。

附加指导：组织根据OMB通知A-130，附录III关于认证信息系统的要求来实施安全证书。在所有的安全认证（授权）决定中，安全证书都是一个重要的因素，并且跨越整个系统开发生存周期。组织在最初的安全认证中对信息系统中所有的安全措施进行评估。根据OMB策略，在最初的认证之后，组织会进行持续的监控（见CA-7），并且每年对一些措施进行评估。组织可以用当年安全认证中获得的评估结果来满足FISMA每年的评估要求（见CA-2）。NIST SP 800-53A中提供了关于安全措施评估的指南。NIST SP 800-37中提供了关于安全证书和认证的指南。相关的安全措施：CA-2，CA-6，SA-11。

ICS附加指导：评估应该由组织授权的称职（具有评估ICS的经验）的评估员来执行和记录。外部审计（比方来自外部管理机构）在该要求范围之外。组织保证评估不影响ICS的功能。在某些情况下，组织认为实施ICS在线测试是不合适或者不可取的

（或者产生负面影响，影响安全性，可靠性），组织应记录下使用复制系统的原因。

增强控制:

(1) 组织使用独立的认证代理或者认证组来执行信息系统安全措施评估。

增强附加指导: 独立的认证代理或者认证组是指能够对组织信息系统进行公平评估的个人或组织。公平是指评估者不存在潜在的或实际的与信息系统的开发、运行或管理命令相关或者与安全措施有效性判定相关的利益冲突。独立的安全认证服务可以从组织内部的其他部门获取也可以通过与组织外部的公共或私立实体签订合同获取。假如信息系统所有人不直接参与合同过程或者不会对认证代理或者认证组织性信息系统安全措施评估产生不良影响，可以认为认证服务是独立的。授权官员根据信息系统的重要性、敏感性和评估对组织操作、财产和人员的最终风险来决定对认证人员独立性的需求程度。由授权官员来决定是否认证人员的独立程度足够保证评估结果有效，而且可以用来指定可靠的、基于风险的决定。在特殊情况下，例如当拥有信息系统的组织很小或者组织结构要求由系统所有者链中负责开发、操作和管理的人员或者授权官员来执行安全措施评估时，可以通过邀请独立专家组验证结果的完整性、一致性和准确性，对评估结果的仔细审核和分析来保证认证过程的独立性。授权官员应该与检察长办公室、高级机关信息安全官员和首席信息官员商量讨论上面所提到的特殊环境下，认证人员独立性判断的潜在含义。

LOW CA-4	MOD CA-4 (1)	HIGH CA-4 (1)

CA-5 实施计划和阶段性成果

控制:组织为信息系统拓展和更新[指定:组织定义的频率]了一个行动计划和里程碑，其阐释了组织结构的计划的、实施的、评估的矫正行为，目的在于修正在安全控制评估中的缺陷，并且去减少或者消除在系统中发现的脆弱性。

附加指导: 行动计划和里程碑是用于正式的授权的安全授权包中的核心文件，与OMB建立的联邦报告要求相一致。行动计划和里程碑的更新是基于来自以下来源的发现: 安全控制评估、安全冲击分析、持续的监控行为。OMB FISMA报告指南中包括行动计划和里程碑的指导。行动计划和里程碑是安全授权包(开发其的目的在于正式的授权)中的核心文件。NIST Special Publication 800-37提供了对于安全证书和信息系统授权的指导性原则。NIST Special Publication 800-30提供了关于风险缩减的指导性原则。

增强控制: 无。

LOW CA-5	MOD CA-5	HIGH CA-5

CA-6 安全授权

控制: 组织在信息系统运行之前授权，并且当系统发生重大改变时更新授权[指定:

组织定义的频率，至少三年一次].上级官员签署并批准该安全授权。

附加指导：OMB Circular A-130，Appendix III中为联邦信息系统的安全授权建立了安全政策。组织结构评估了被运用在信息系统中的安全控制，并且支持安全授权。用于支持安全授权的安全评估被称为安全认证。信息系统的安全授权并不是一个静态过程。通过采用一个全面的持续监控过程（认证授权过程的第四和最后一项），授权包中包含的重要信息（系统安全计划，系统评估报告，实施计划和阶段性成果）得到持续更新，从而为授权官员和信息系统所有者提供了信息系统安全的最新状态。为了减小三年重授权过程的管理负担，授权官员尽可能的最大程度采用正在进行的持续监控过程的结果作为得出重授权决定的基础。NIST Special Publication 800-37提供了对于安全证书和信息系统授权的指导性原则。相关的安全措施：CA-2，CA-4，CA-7。

增强控制：无。

LOW CA-6	MOD CA-6	HIGH CA-6

CA-7 持续监控

控制：组织结构监控基于运行基础之上的信息系统的安全控制。

附加指导：持续监控包括配置管理和对信息系统组建的管理，系统改变产生的安全影响的分析，持续的安全措施评估和状态汇报。在初始的安全授权中，组织对信息系统中所有的安全措施进行评估。在最初的授权后，根据OMB的策略，组织在持续的监控中每年对一部分措施进行评估。合适的安全措施的选择根据：(i) FIPS 199 信息系统安全等级；(ii) 组织保护信息系统所采用的具体安全措施；(iii) 组织用来决定信息系统中安全措施有效性的信任等级。组织首先建立选择条件，然后从信息系统中选择一部分安全措施用来评估。组织为措施监控制定进度表，保证每次评估的措施的范围都是有效的。那些对于保护信息系统至关重要的措施至少每年评估一次。其他的措施至少要在3年的授权周期中被评估过一次。组织可以用持续的监控中当年的安全认证中的评估结果来满足FISMA的评估要求（见 CA-2）。该措施与监控信息系统配置改变很相关。有效的持续监控项目可以有效地更新信息系统安全计划，安全评估报告和实施计划与阶段性成果—他们是安全授权包中的三篇基本文档。严格的持续监控可以显著减少信息系统重授权需要付出的努力。NIST Special Publication 800-37提供了对于安全证书和信息系统授权的指导性原则。NIST Special Publication 800-53A对安全控制评估提供了指导性意见。相关的安全措施：CA-2，CA-4，CA-5，CA-6，CM-4。

增强控制：

(1) 组织使用独立的认证代理或者认证组来对持续运行的系统的安全措施进行监控。

增强附加指导：在系统持续运行的监视过程中，通过要求独立的认证代理或者认证

组在三年的授权周期中对所有的安全措施进行评估，组织可以将持续的安全措施的评估值扩展或最大化。

LOW CA-7	MOD CA-7	HIGH CA-7

类： 配置管理(CM)
CLASS：OPERATIONAL

CM-1 配置管理策略和规程

控制：组织开发、发布、周期性回顾/更新以下内容：(I)一个正式的、有说明文件的配置管理策略，用于解决目的、范围、角色、责任、管理委托、组织实体间的协调和顺应性)；(II)正式的、有说明文件的规程用于推进配置管理策略和关联的配置管理控制的实施。

附加指导：配置管理策略和规程符合联邦法律、命令、政策、规范、标准和指导性原则的精神。配置管理策略可能属于总体信息安全策略的一部分。可以针对总的安全项目开发配置管理规程，也可以应需求针对特殊的信息系统。NIST Special Publication 800-12提供了对于安全策略和规程的指导性原则。

增强控制：无。

LOW CM-1	MOD CM-1	HIGH CM-1

CM-2 基线配置

控制：组织去开发、同时形成文件并且维护了一个当前的基线的信息系统的配置的清单。

附加指导：该措施为信息系统建立基线配置。基线配置中提供关于信息系统架构中特殊部件的组成（如，基站或笔记本电脑中升级补丁之类的标准软件负载）和部件逻辑位置的相关信息。如果需要的话，基线配置中还可以提供系统建立的相关说明，这些说明是为了任务需要/目标而整理成文本的。信息系统的配置与联邦企业架构相一致。相关的安全措施：CM-6，CM-8。

增强控制:

(1) 组织更新基线配置作为信息系统部件安装的一个部分。

(2) 组织应用自动化的机制去维护一个最新的、完整的、精确的、便于应用的信息系统基线配置。

LOW CM-2	MOD CM-2 (1)	HIGH CM-2 (1) (2)

CM-3 配置改变的控制

控制：组织授权、记录并控制对信息系统的改变。

附加指导：组织使用组织认可的章程（例如特许的配置控制板）来管理信息系统的配置改变。配置改变控制包含系统性的提议、合理性确认、执行、测试/评估、回顾

及相应于建议的改变的部署，例如升级和修改。配置改变控制包括对信息技术产品（例如，操作系统，防火墙，路由器）的配置设置改变。组织在配置改变控制过程中包含紧急改变，包括漏洞补救导致的改变。认可对信息系统实施修改包括对修改进行安全分析所得到的成功结果。组织审核与信息系统配置改变相关的行为。相关的安全措施：CM-4，CM-6，SI-2。

ICS附加指导：NIST SP 800-82中提供了ICS的配置改变措施方面的指南。

NIST SP 800-82 ICS特别推荐与指南：对可能会影响ICS网络安全的所有改变作风险评估，如果需要的话，也对策略和章程进行修改。ICS网络的配置文档必须及时更新。

增强控制：

(1) 组织使用自动机制达到如下目的：(i)以文本形式说明对信息系统的建议的改变；(ii)通知审批的有关当局；(iii)突出没有及时获得的批准；(iv)在得到必要的回复建议之前防止产生变化；(v)阐释对信息系统的整体性改变。

ICS增强附加指导：在某些情况下，组织认为实施自动机制是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

(2) 在将改变（如补丁和升级）安装到正在运行的ICS上之前，组织测试，验证并记录他们。

ICS增强附加指导：组织保证测试并不影响ICS的功能。测试者完全了解公司信息与ICS安全策略、步骤以及与特别的设备或过程相关的具体的健康，安全和环境风险。在评估开始之前，ICS产品可能需要离线，并且复制到可行的设备（盘区）？将如ICS必须离线评估，那么可以将评估安排在任何可能的计划好的ICS停机阶段。在某些情况下，组织认为实施ICS在线测试是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下使用复制系统的原因。

LOW Not Selected	MOD CM-3	HIGH CM-3 (1)

CM-4 监视配置改变

控制：组织结构监视信息系统的变化，并且作安全影响分析以便确定改变的效果。

附加指导：在实施改变之前，作为改变认可过程的一部分，组织分析改变对信息系统潜在的安全影响。在对信息系统进行改变后（包括升级和修改），组织对安全特征进行检察，保证其功能可靠。组织审查与信息系统配置改变相关的行为。监控配置改变与执行安全影响分析是与信息系统持续的安全措施评估相关的两个重要部分。相关的安全措施：CA-7。

ICS附加指导：组织应考虑ICS安全状态与安全措施的相关性。

增强控制：无。

LOW Not Selected	MOD CM-4	HIGH CM-4

CM-5 对改变的访问限制

控制：组织(i)批准个人访问特权，强制执行与信息系统改变相关物理和逻辑访问控制；(ii)产生、保留并审核反应这些改变的记录。

附加指导：计划的或非计划的对信息系统硬件、软件和固件的修改会对整个系统的安全产生重大的影响。因此，只有有资格的被授权的个人才能对这些信息系统部件进行访问来进行升级和修改。

增强控制：

(1) 组织结构使用自动的机制去强制进行访问控制，并且支持对强制性行为的审计。

ICS增强附加指导：在某些情况下，组织认为实施自动机制是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

LOW Not Selected	MOD CM-5	HIGH CM-5 (1)

CM-6 配置设置

控制：组织(i)为信息系统中所采用的信息技术产品建立强制的配置设置；(ii)将信息技术产品的安全设置配置到与操作要求一致的最严格的模式；(iii)以文本形式记录配置设置；(iv)在信息系统的所有部件上强制执行配置设置。

附加指导： 配置设置是组成信息系统的信息技术产品的配置参数。组织根据策略和章程监控对配置设置的改变。OMB FISMA报告的规程中提供了联邦信息系统配置需求的相关指南。NIST Special Publication 800-70中提供了关于组织信息系统中信息技术产品配置设置的相关指南。相关的安全措施：CM-2，CM-3，SI-4。

增强控制：

(1) 组织结构运用自动的机制去集中的管理、应用和验证配置设置。

ICS增强附加指导：在某些情况下，组织认为实施自动机制是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

LOW CM-6	MOD CM-6	HIGH CM-6 (1)

CM-7 最小功能

控制：组织设定信息系统只提供最基本的功能，并组织和（或）限制如下功能、端

口、协议和（或）服务的使用[制定：组织定义的被禁止和/或限制的功能、端口、协议和（或）服务]。

附加性指导意见： 信息系统可以提供大量的功能和服务。一些缺省提供的功能和服务对于制成基本的组织操作（如，重要的任务和功能）是没有必要的。而且，有时由信息系统的单个部件提供多种服务很方便，但是这样会增加限制单个部件所提供的服务而带来的风险。更切实可行的方法是，限制每个设备只提供一个功能（如，email服务器，网页服务器）。信息系统或者单个部件所提供的功能和服务应当仔细审查，从而判断出那些功能和服务应该被关闭（如，VoIP，即时消息，FTP，HTTP，文件共享）。

ICS附加指导：组织应考虑关闭ICS组件上不使用或没必要的物理和逻辑端口（如，USB，PS/2，FTP）以阻止委授权的硬件连接（如小型驱动？，按键记录器？）。

增强控制:

(1) 组织审查信息系统[制定：组织定义的频率]，识别并关闭不必要的功能、端口、协议和（或）服务。

LOW Not Selected	MOD CM-7	HIGH CM-7 (1)

CM-8 信息系统部件目录

控制：组织开发，存档并维护最新的信息系统部件目录和相关的所有者信息。

附加指导：组织判断对目录中的信息系统部件的管理（跟踪和报告）粒度层次。信息系统部件目录中包括任何组织认为可以有效呈现特性的必要信息（例如，厂商，型号，序列号，软件许可信息，系统/部件所有人）。部件目录与信息系统的授权边界相一致。相关的安全措施：CM-2，CM-6。

增强控制:

(1) 组织将升级信息系统部件目录作为部件安装的一部分。

(2) 组织使用自动机制维护最新的、完整的、精确的并且随时可用的信息系统部件目录。

LOW CM-8	MOD CM-8 (1)	HIGH CM-8 (1) (2)

类： 应急计划(CP)
CLASS：OPERATIONAL

CP-1 应急计划的策略和章程

控制：该组织制定、发布、周期性地检查与更新：（i）一份正式存档的应急计划的策略，其标明了目的、范围、角色、责任、管理委托、各组织间的协调和一致。(ii)正式存档的各种章程，目的是推动应急计划策略与应急计划相关措施的执行。

附加指导：应急计划的策略和章程要与现有生效的法律、指示、政策、规则、标准和指导建议保持一致。应急计划策略可作为该组织通用信息安全策略的一部分。需要时，可以为一般的安全章程或特殊信息系统制定应急计划章程。NIST特别报告800-34提供了应急计划的指导建议。NIST特别报告800-12提供了安全策略和章程的指导建议。

增强控制：无。

LOW CP-1	MOD CP-1	HIGH CP-1

CP-2 应急计划

控制：该组织制定并执行信息系统的应急计划，包括应急的人员角色、责任、个人联系信息和当破坏或故障发生时恢复系统的步骤。该组织的设计人员检查核准应急计划，并拷贝多份计划分发给关键事故责任人。

附加指导：无。

ICS附加指导：组织应为中断和失败分类制定偶然事件计划。当在ICS内部或与操作设备通信过程中发生处理失败时，ICS组件应执行某些预置措施，如：

(1) 向操作者发出失败警告，不采取措施。

(2) 向操作者发出失败警告，并安全关闭工业进程。

(3) 保留失败前最后的操作设置。

NIST SP800-82中为ICS失败模式提供了指南。

增强控制：

(1) 组织配合负责相关计划的组织单元来进行应急计划的制订。

增强附加指导：相关的计划的事例包括商业应急计划、灾难恢复计划、连续作业计划、商业恢复计划、事件响应计划和紧急行动计划。

(2) 组织制定性能计划是为了在出现紧急情况时，系统仍具有信息处理，通信和环境支持的能力。

LOW CP-2	MOD CP-2 (1)	HIGH CP-2 (1) (2)

CP-3 应急培训

控制：该组织根据人员担任信息系统的应急角色和责任的不同进行培训，并提供复习进修的培训（任务：该组织自定义时间周期，至少一年一次）。

附加指导：无。

增强控制：

(1) 组织模拟事件以配合应急培训，使得人员在危难时刻具备高效的应对能力。

(2) 组织使用自动化机制提供更加全面真实的培训环境。

LOW Not Selected	MOD CP-3	HIGH CP-3 (1)

CP-4 应急计划测试

控制：组织(i)测试（或演习）信息系统的应急计划（指定：组织定义的时间周期，至少一年一次）用来确定计划的有效性和该组织执行计划的准备情况（指定：组织定义的测试和演习）；(ii)对应急计划测试/演习的结果审查并对计划进行修正。

附加指导：有多种方式可以测试和（或）演习应急计划并确定潜在的弱点（例如，应急计划的全面测试、功能性演习）。应急计划测试/演习的深度和精细程度随着FIPS199信息系统影响等级的增加而提高。紧急计划测试/演习中还应包括按照计划所执行的紧急操作对组织运行、财产（如操作能力下降）和人员的影响程度的判断。NIST SP 800-84中提供了信息技术计划能力的测试、培训和演习项目的相关指南。

增强控制：

(1) 组织配合负责相关计划的组织单元来进行应急计划的测试和（或）演习。

增强附加指导：相关的计划的事例包括商业应急计划、灾难恢复计划、连续作业计划、商业恢复计划、事件响应计划和紧急行动计划。

(2) 该组织在备用处理设备上测试/执行应急计划，使应急人员熟悉设备和各个可用的资源，并以此评估该设备支持应急操作的性能。

(3) 该组织使用自动化机制，通过提供对紧急事件更全面的覆盖，选择更实际的测试/演习场景和环境，更有效的强调信息系统和支撑认识，更加完全有效地对应急计划进行测试/演习。

LOW Not Selected	MOD CP-4 (1)	HIGH CP-4 (1) (2)

CP-5 应急计划更新

控制: 组织复查信息系统的应急计划(指定: 组织定义的时间周期, 最少一年一次), 并且根据系统和组织上的改变或在计划实施执行或测试中遇到的问题, 对计划进行修订。

附加指导: 组织的改变包括信息系统所执行的任务、功能或事务处理上的改变。组织将这些改变通知负责各相关计划(商业应急计划、灾难恢复计划、连续作业计划、商业恢复计划、事件响应计划、紧急情况相应计划)的部门。

增强控制: 无

LOW CP-5	**MOD CP-5**	**HIGH CP-5**

CP-6 备用存储设备

控制: 组织标识备用存储设备并启动必要的协议允许存储信息系统备份信息。

附加指导: 信息系统备份的频率和将备份数据传输至备用存储设备(如果已经指定了)的速率要与组织的恢复时间目标和恢复点目标相一致。

增强控制:

(1) 备用存储设备与主存储设备实施物理隔离以防止受到同样灾难的破坏。

(2) 组织对备用存储设备进行配置, 保证其及时有效的进行恢复操作。

(3) 该组织要指出当发生区域性破坏或灾难时, 备用存储设备潜在的问题, 并明确补救措施。

LOW Not Selected	**MOD CP-6 (1) (3)**	**HIGH CP-6 (1) (2) (3)**

CP-7 备用处理设备

控制管理: 组织对备用处理设备进行标识, 并当主处理设备处理能力不足时, 在[指定: 组织定义的时间]内, 允许信息系统恢复关键指令/商业功能操作。

附加指导: 在组织规定的时间内恢复操作所需的设备和供应要么已经在备用位置上可用, 要么可以通过规定途径传输到备用设备上。恢复信息系统操作的时间表要与系统建立的恢复时间目标相一致。

ICS附加指导: 在某些情况下,组织认为实施备用处理站点是不合适或者不可取的(或者产生负面影响, 影响安全性, 可靠性), 组织应记录下不采用措施的原因, 在系统安全计划中记录合适的补偿安全措施, 并加以实施。相关的安全措施: PL-2。

控制增强:

(1) 备用处理设备与主处理设备实施物理隔离以防止受到同样灾难的破坏。

(2) 该组织要指出当发生区域性破坏或灾难时，备用存储设备潜在的问题，并明确补救措施。

(3) 备用处理设备根据组织的可用性需求支持服务优先级功能。

(4) 组织对备用处理设备进行配置保证它随时可用，并能支持基本功能。

LOW Not Selected	MOD CP-7 (1) (2) (3)	HIGH CP-7 (1) (2) (3) (4)

CP-8 通信服务

控制：组织对支持信息系统通信的主备设备进行标识，并当主通信设备处理能力不足时，在[指定：组织定义的时间]内，允许信息系统恢复关键指令/商业功能操作。

附加指导：如果主通信服务和（或）备用通信服务采用电信载波，组织要求所有用于国家安全紧急预备方案的通信服务都具有TSP（通信服务优先级）。（有关TSP计划的详尽解释请登录网站*http：//tsp.ncs.gov*）

控制增强：

(1) 主通信服务和备用通信服务的协议应包含服务供应优先级功能，优先级根据该组织的可用性需求指定。

(2) 备用通信服务系统与主通信服务系统不存在同样的单点故障。

(3) 组织要求备用通信服务系统与主服务系统是完全隔离的，以免遭受同样灾难的破坏。

(4) 组织要求主副通信服务提供商都要有适当的应急计划。

LOW Not Selected	MOD CP-8 (1) (2)	HIGH CP-8 (1) (2) (3) (4)

CP-9 信息系统备份

控制：组织[指定：组织定义的频率]对信息系统中的用户级和系统级信息（包括系统状态信息）进行备份，并且对备份信息进行保护。

附加指导：信息系统备份的频率和将备份数据传输至备用存储设备（如果已经指定了）的速率要与组织的恢复时间目标和恢复点目标相一致。根据存储在备份介质上的信息的类型和FIPS199影响等级，尽管完整性和可用性是系统备份信息主要关注的特性，保护备份信息以免非法泄露也非常的重要。组织风险评估指导对备份信息的加密。保护传输中的系统备份信息不在该措施的考虑范围内。相关的安全措施：MP-4，MP-5。

增强控制:

(1) 组织[指定: 组织定义的频率]对备份信息进行测试以确保介质可靠性和信息的完整性。

(2) 作为应急计划测试的一部分，组织在恢复信息系统功能时有选择的使用备份信息。

(3) 组织将操作系统和其他重要信息系统软件的备份副本存储在隔离设备上或者没有配置操作软件的存储器中。

(4) 组织对系统备份信息进行保护，使其不被非法修改。

附加指导: 组织采用合适的机制（如: 数字签名，加密散列）对信息系统备份的完整性进行保护。对系统备份信息进行机密性保护不在该措施的控制范围。相关的安全措施: MP-4，MP-5。

LOW CP-9	MOD CP-9 (1) (4)	HIGH CP-9 (1) (2) (3) (4)

CP-10 信息系统恢复与重建

控制管理: 组织使用一些机制支持信息系统的恢复与重建，使之在破坏和故障后，能够恢复到系统原有的状态。

附加指导: 安全地将信息系统恢复与重建到原有的状态意味着所有系统参数（包括默认值或该组织自定义的值）都将被设置为安全值，补丁要重新安装，安全相关的配置要重新设置，系统文件和程序可用，应用软件和系统软件要重装，加载最近一次安全备份上面的信息，此时系统需要进行全面测试。

ICS附加指导: 在某些情况下，组织认为实施措施或措施加强是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施: PL-2。

控制增强:

(1) 该组织将信息系统的完全恢复与重建作为应急计划测试的一部分。

LOW CP-10	MOD CP-10	HIGH CP-10 (1)

类： 标识与鉴别(IA)
CLASS：TECHNICAL

IA-1 标识与鉴别的策略和章程

控制: 该组织制定、发布、周期性地检查与更新: （i）一份正式存档的鉴别与认证策略，其标明了目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及顺从关系。(ii) 正式存档的各种章程（用来促进鉴别与认证政策的执行），以及相关的认证和鉴别控制。

附加指导: 鉴别与认证的策略和章程要与下述文档保持一致: （i）FIPS201和特别版的800-73，800-78和800-76; （ii）其他现有生效的法律、可执行命令、指令、政策、规则、标准和指导。鉴别和认证策略可以作为组织通用信息安全策略的一部分。在需要的时候，可以为普通安全程序或特殊的信息系统开发鉴别和认证章程。NISF特别版800-12提供了安全策略和章程方面的指导。NIST特别版800-63提供了远程电子认证方面的指导。

增强控制: 无。

LOW IA-1	MOD IA-1	HIGH IA-1

IA-2 用户标识与鉴别

控制: 信息系统唯一标识和鉴别用户（或处理用户的行为）。

附加指导: 除了那些身份明确以及由组织依照安全控制AC-14进行证明的访问之外，用户的其他所有访问都要被唯一的鉴别和认证。用户身份的认证由用户密码，记号，生物特征或由以上多方式的混合认证来完成。NIST SP 800-63适用于对信息系统本地和远程的访问。远程访问是由用户(或信息系统) 通过外部的，非组织控制的网络(如Internet)对组织信息系统的任何形式的访问，本地访问是由用户(或信息系统) 通过内部的，组织控制的网络(如本地局域网)或不通过网络而直接由设备接入的对组织信息系统的任何形式的访问。除非特别声明了一种更加迫切的增强控制方案，NIST SP 800-63等级1将适用于所有的本地和远程信息系统的访问认证。FIPS201和SP 800-73，800-76和800-78为联邦雇员和承包人使用唯一鉴别和认证机制，详细阐明了一种个人身份确认标准。除了在信息系统级别上(如在系统登陆上网)鉴别和认证用户，鉴别和认证机制在应用级别也同样适用，如在必要时，为组织提供附加的信息安全。

为了与OMB策略和电子认证电子政府法案保持一致，也可能要求公共用户对联邦信息系统的认证访问，用以保护非公共的或私人相关的信息。按照OMB便函 04-04 ，电子认证风险评估指导被用于决定NIST SP 800-63关于IA-2控制和增强控制对此类访问的附加需求。在平衡以下两种需求时(确保对该信息和信息系统公共访问的易用性需求和保护组织操作，组织资产和个体的需求)可测量性，实用性，和安全问题将被同时考虑。相关安全控制有: AC-14，AC-17。

ICS附加指导：当用户功能可以推为同一类（比如控制室操作员）时，用户身份识别与认证可以基于角色，基于组或者基于设备。对于一些ICS，操作员及时相应很重要。身份识别与认证要求绝不能影响ICS的本地紧急相应。对这些系统的访问可以通过合适的物理安全措施来限制。在某些情况下，组织认为实施措施或措施加强是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。NIST SP 800-82中提供了关于ICS用户身份识别与认证相关的指南。相关的安全措施：PL-2。

NIST SP 800-82 ICS特别推荐与指南：目前ICS访问采用的认证方式包括但不局限于口令认证，请求/响应认证，令牌认证和生物信息认证。这几种认证在使用的过程中要考虑的是：

(1) 口令认证：口令的选择要平衡长度、强度、操作难度等多个因素；密码的熵要高；对于没有物理保护的远程设备要双因素认证；主密码要保证安全；私人密码要经常更换，主密码的修改要有授权而且要保留记录；对于一些重要的系统，要仔细考虑是否要采用口令，以防止在紧急情况下，工作人员由于慌张导致的响应速度减慢；口令传输要加密，不能以明文出现在网络中；对于网络服务认证，用C/R或公钥比较合适。

(2) 请求/响应认证：不用像password那样在网络上直接传输，因此比password安全性高，但是由于协议语句的增加，导致响应速度降低。

(3) 令牌认证：由于令牌可能会丢失，因此将令牌作为双因素认证中的一部分，用于从ICS防火墙外部访问ICS应用很合适。

(4) 生物信息认证：生物信息不会丢失，可以和令牌结合起来作为双因素认证，但是由于生物信息只能在现场使用，所以适合用于控制室的访问控制。

增强控制：

(1) 信息系统对远程系统访问使用多方式混合认证，此为NIST SP 800-63(选择：组织自定义的等级3，等级3使用一种硬件认证设备，或等级4)条例。

(2) 信息系统对本地系统访问使用多方式混合认证，此为NIST SP 800-63(选择：组织自定义的等级3，或等级4)条例。

(3) 信息系统对远程系统访问使用多方式混合认证，此为NIST SP 800-63等级4条例。

ICS增强附加指导：对于措施加强1，2和3，只有在必要的，经过批准和认证的情况下，本地或者远程用户才允许访问ICS组件。如附录B中所定义的，远程访问是指用户或某一信息系统通过外部非组织控制的网络来对组织信息系统进行访问。对于ICS，组织就是控制系统的所有者/操作者。因此，ICS远程访问是指从控制系统所有者/操作者所定义的系统边界外部对ICS进行访问。组织应考虑对本地和远程用户对ICS访问的多参数认证。NIST SP 800-82中提供了ICS远程访问的相关指南。

NIST SP 800-82 ICS特别推荐与指南：远程访问采用加密的协议，并且采用多因素认证。可以通过企业网内的系统与控制网络进行通信，但是要在控制网络防火墙上实

现双因素认证。

LOW IA-2	MOD IA-2 (1)	HIGH IA-2 (2) (3)

IA-3 设备标识与鉴别

控制：信息系统在建立连接之前鉴别并认证特定的设备。

附加指导：信息系统或者使用共享信息(如介质访问控制MAC)或传输控制协议/网络协议(TCP/IP)地址)，或者组织认证的方案(如IEEE802.1x和扩展认证协议(EAP)或在扩展认证协议EAP-传输层安全TLS认证服务范围)来鉴别和认证局域网或广域网的设备。设备认证机制所需的增强控制是由FIPS199 影响级别高，需要更强认证的信息系统的安全分类来决定的。

ICS附加指导：在某些情况下，组织认为实施设备身份识别与认证是不合适或者不可取的（比如串行设备），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：无。

LOW Not Selected	MOD IA-3	HIGH IA-3

IA-4 标识符管理

控制：该组织通过以下几种方式管理用户标识符：(i)唯一识别每一个用户；(ii)验证每一个用户的身份；(iii)从适当的官方机构接收授权许可发放一个用户标识符；(iv)将用户标识符发放给预期的那一方；(v)在组织自定义的一个时间段内，用户停止活动时，注销用户标识符；(vi)归档用户标识符。

附加指导：标识符管理不适合于共享的信息系统账号（例如guest用户和匿名用户）。FIPS 201和SP 800-73，800-76和800-78为联邦雇员和承包人使用唯一鉴别和授权机制，详细阐述了一种人员身份识别方案。

ICS附加指导：当用户功能可以推为同一类（比如控制室操作员）时，用户身份识别与认证可以基于角色，基于组或者基于设备。对于一些ICS，操作员及时相应很重要。身份识别与认证要求绝不能影响ICS的本地紧急相应。对这些系统的访问可以通过合适的物理安全措施来限制。在某些情况下，组织认为实施措施或措施加强是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。NIST SP 800-82中提供了关于ICS用户身份识别与认证相关的指南。相关的安全措施：PL-2。

NIST SP 800-82 ICS特别推荐与指南：目前ICS访问采用的认证方式包括但不局限于口令认证，请求/响应认证，令牌认证和生物信息认证。这几种认证在使用的过程中要考虑的是:

(1) 口令认证：口令的选择要平衡长度、强度、操作难度等多个因素；密码的熵要高；对于没有物理保护的远程设备要双因素认证；主密码要保证安全；私人密码要经常更换，主密码的修改要有授权而且要保留记录；对于一些重要的系统，要仔细考虑是否要采用口令，以防止在紧急情况下，工作人员由于慌张导致的响应速度减慢；口令传输要加密，不能以明文出现在网络中；对于网络服务认证，用C/R或公钥比较合适。

(2) 请求/响应认证：不用像password那样在网络上直接传输，因此比password安全性高，但是由于协议语句的增加，导致响应速度降低。

(3) 令牌认证：由于令牌可能会丢失，因此将令牌作为双因素认证中的一部分，用于从ICS防火墙外部访问ICS应用很合适。

(4) 生物信息认证：生物信息不会丢失，可以和令牌结合起来作为双因素认证，但是由于生物信息只能在现场使用，所以适合用于控制室的访问控制。

增强控制：无。

LOW IA-4	MOD IA-4	HIGH IA-4

IA-5 认证设备管理

控制：该组织通过以下方式来管理信息系统的认证设备：(i)定义最初的认证设备内容；(ii)为最初认证设备的分发、丢失/泄漏的或损坏的、废除的认证设备建立管理程序；(iii)在信息系统安装更改时修改默认的认证设备;(iv)定期地更改或更新认证设备。

附加指导：信息系统认证设备包括：如标记，PKI证书，生物特征，口令，密钥卡。用户采取合理的措施来保护他们鉴别设备，包括保存维护好他们的个人鉴别设备，不转借或共享给他人，一旦丢失或外泄则立刻上报。对基于口令的认证方式，信息系统要：(i)保护口令，当存储和传输时，不会被未授权的人公开、更改；(ii)输入口令时禁止口令明文显示；(iii)实施口令自动期满；(iv)禁止口令反复使用特殊数字；对基于PKI的认证方式，信息系统要：(i)通过为可信任对象创建证明路径来确认证书;(ii)建立通讯私钥的用户控制;(iii)将用户帐户与认证实体相对应。按照OMB策略和相关的电子认证动机，公共用户访问联邦信息系统(和相关认证设备管理)的认证也有可能被要求使用，目的是保护非公共的或私人相关的系统。FIPS 201和SP 800-53，800-76和800-78中指明了将PIV用于标识联邦员工和承包人。NIST SP 800-63提供了远程电子认证相关的指南。

ICS附加指导：许多ICS设备和软件都是采用厂商缺省认证证书以完成初始安装和配置。然而，厂商的缺省认证证书经常很容易得到，从而造成了巨大的安全风险，应该更换。认证应该是基于角色的，基于组的或者基于设备的。在某些情况下，组织认为实施措施是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并

加以实施。NIST SP 800-82中提供了关于ICS认证设备管理相关的指南。相关的安全措施：PL-2。

NIST SP 800-82 ICS特别推荐与指南：对于口令认证，主密码要保证安全；私人密码要经常更换；对于令牌认证，令牌一定要妥善保管。

增强控制：无。

LOW IA-5	MOD IA-5	HIGH IA-5

IA-6 鉴别设备的反馈消息

控制： 在认证过程中，信息系统隐藏了认证信息的反馈消息，为了保护信息不被未授权的个体利用。

附加指导：信息系统的反馈消息并不会向未授权用户泄漏认证信息。当用户键入口令时显示星号，就是隐藏认证信息反馈消息的一个例子。

增强控制：无。

LOW IA-6	MOD IA-6	HIGH IA-6

IA-7 密码模块认证

控制：为了对密码模块进行认证，信息系统使用一些符合可适用法律，可执行命令、指令、策略、规则、标准和指导的要求的认证方法。

附加指导：密码模块认证中生效的联邦标准为FIPS140-2(修正版)。由NIST密码模块确认程序(包括FIPS140-1，FIPS140-2和后来修改版)发布的确认证书仍然有效，并且那些模块仍然可以继续使用和购买，直到该确认证书被明确废除为止。关于使用有效密码系统的附加信息可以在*http://csrc.nist.gov/cryptval*网站上得到。

ICS附加指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。

增强控制：无。

LOW IA-7	MOD IA-7	HIGH IA-7

类： 事件响应(IR)
CLASS：OPERATIONAL

IR-1 事件响应策略和章程

控制管理：该组织制定、发布、周期性地检查与更新：（i）一份正式存档的事件响应策略，其标明了目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及顺从关系。(ii)正式存档的各种章程，用来促进事件响应策略和相关事件响应控制的执行。

附加指导：事件响应策略和章程要与现有生效的法律、可执行命令、指令、政策、规则、标准和指导建议保持一致。事件响应策略可作为该组织通用信息安全策略的一部分。需要时，可以为总的安全程序或特殊信息系统制定应急计划章程。NIST特别报告800-12提供了安全策略和章程的指导建议。NIST特别报告800-61提供了关于事件处理和报告的指导建议。NIST特别报告800-83提供了对恶意软件的事件处理和阻止方面的指导建议。

增强控制：无。

LOW IR-1	MOD IR-1	HIGH IR-1

IR-2 事件响应培训

控制管理：该组织根据个人在信息系统中事件响应中的角色和职责进行培训，并提供复习进修的培训（任务：该组织自定义时间周期，至少一年一次）。

附加指导：无。

控制增强：

(1) 该组织模拟事件以配合事件响应培训，使得人员在危难时刻具备高效的应对能力。

(2) 该组织使用自动化机制提供更加全面真实的培训环境。

LOW Not Selected	MOD IR-2	HIGH IR-2 (1) (2)

IR-3 事件响应测试和演习

控制管理：该组织测试和演习信息系统的事件响应能力[指定：组织自定义的时间周期，至少一年一次]使用[指定：组织自定义的测试和演习]来决定事件响应效率并归档其结果.

附加指导：NIST SP 800-84提供了对信息技术计划和能力关于测试、培训、演习程序的指导建议.

增强控制:

(1) 该组织使用自动化机制,使得更加彻底有效地测试或演习事件响应能力.

增强附加指导:自动机制能提供更加彻底有效的测试或演习的能力,提供覆盖面更完全的事件响应问题,选择更加真实的测试/演习场景和环境,以及更加有效的突出响应能力.

LOW Not Selected	MOD IR-3	HIGH IR-3 (1)

IR-4 事件处理

控制管理: 当安全事件发生时, 该组织实施事件处理的能力, 包括准备、检测、分析、遏制、根除和恢复等方面。

附加指导: 事件相关的信息可以从以下各种资源中获得,包括(但不仅限于)审计监视、网络监视、物理访问监视以及用户/管理员报告.

该组织将目前事件处理行为中总结的经验教训, 与相应的事件响应章程及其实施有机结合起来。相关安全控制: AU-6, PE-6.

增强控制:

(1) 该组织使用自动化机制以支持事件处理过程。

LOW IR-4	MOD IR-4 (1)	HIGH IR-4 (1)

IR-5 事件监控

控制管理: 该组织跟踪并记录正在进行的信息系统安全事件。

附加指导: 无。

增强控制:

(1) 该组织使用自动化机制来帮助跟踪安全事件, 并帮助采集与分析事件信息。

LOW Not Selected	MOD IR-5	HIGH IR-5 (1)

IR-6 事件报告

控制管理: 该组织向适当的负责人及时报告事件信息。

附加指导: 上报事件信息的类型、这些报告的内容和时间、指定的上报负责人或组织的列表要与现有的法律、指示、政策、规则、标准和指导建议保持一致。组织的

官员在一个特定时间段(该时间段是由US-CERT关于联邦计算机安全事件处理的操作概念中指定的)，通过*http://www.us-cert.gov*网站,向美国计算机紧急事件预备队报告计算机安全事件.除了事件信息以外,信息系统的弱点和易攻击点也要及时地向适当的组织官员上报用以阻止安全事件发生.NIST SP 800-61提供了上报事件的指导建议.

ICS附加指导：每个组织都应奖励报告标准，包含可以通过合适途径共享的信息。US-CERT的ICS安全中心的网址是http://www.uscert.gov/control_stystems/。NIST SP 800-82中提供了ICS事故报告的相关指南。

NIST SP 800-82 ICS特别推荐与指南：如果响应计划中包含事件报告要求，那么应该指明报告的对象是谁，联系对象的电话是多少。

增强控制:

(1) 该组织使用自动化机制来帮助安全事件的上报。

LOW IR-6	MOD IR-6 (1)	HIGH IR-6 (1)

IR-7 事件响应支持

控制管理：该组织提供事件响应支持资源，给信息系统的使用者提供建议和帮助来处理或上报安全事件。这些支持能力是构成该组织的事件响应能力不可或缺的一部分。

附加指导：组织中事件响应支持资源的可能的执行方案包括帮助台或辅助团队以及在必要时，辩论练习访问服务.

增强控制:

(1) 该组织使用自动化机制来增强事件响应信息及其支持的有效性。

LOW IR-7	MOD IR-7 (1)	HIGH IR-7 (1)

类： 维护(MA)
CLASS： OPERATIONAL

MA-1 系统维护策略和章程

控制：组织开发、发布、定期回顾/升级：(i)一份正式存档的信息系统维护策略，其标明了目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及顺从关系。(ii)正式存档的各种章程，用来促进信息系统维护策略和相关系统维护控制的执行。

附加指导： 信息系统维护策略和章程要与现有生效的法律、可执行命令、指令、政策、规则、标准和指导建议保持一致。信息系统维护策略可作为该组织通用信息安全策略的一部分。需要时，可以为一般的安全程序或特殊信息系统制定应急计划章程。NIST特别报告800-12提供了安全策略和章程的指导建议。

增强控制：无。

LOW MA-1	MOD MA-1	HIGH MA-1

MA-2 定期维护

控制管理：组织确定计划、执行、用文件记载并回顾信息系统构成部件中的日常预防性的和例行的维护（包括维修）记录，这些记录要与厂商/卖方的说明书和/或组织的需求一致。

附加指导：所有常规的维护和维修操作都是被控制的；无论是现场操作或是远程操作，无论该设备是现场服务或是被移动到其他场所。组织官员只有在必要的时候才会批准将信息系统或信息系统部件移动到其他地方。

如果信息系统或系统部件需要场外修补的话，组织将从使用被认可章程的相关介质中移除所有的信息。在信息系统的维护工作完成后，组织检测所有潜在的会产生影响的安全控制以确保这些控制仍恰当地运行。

增强控制：

(1) 组织保存的对信息系统的维护日志包括：(i)维护的日期和时间；(ii)执行维护操作的个体名字；(iii)如果有必要，也包括陪同的名字；(iv)对执行的维护操作的描述。 (v) 已移动的和替换的设备列表（包括鉴别数字，如果可行的话）

(2) 组织使用自动化的机制来制定并指导维护，并为所有的维护操作创建最新的，精确的，完整的和可用的记录，这些记录应该是必须且完整的。

LOW MA-2	MOD MA-2 (1)	HIGH MA-2 (1) (2)

MA-3 维护工具

控制：组织批准、控制和监视信息系统维护工具的使用，并持续的维护该工具。

附加指导：该控制的目的在于为引入信息系统的硬件和软件打上标记，尤其针对诊断/修补操作（如，为某种专门维护行为而引进的软件或硬件分组嗅探器）。那些可能支持信息系统维护的硬件或软件部件，虽然也是系统的一部分，但并不包含在该控制中。（如，软件命令“ping”，“ls”，“ipconfig”，或执行监视以太网转换端口的硬件或软件）

增强控制：

(1) 组织审查所有由维护人员因为明显不恰当的修改而投入设施的维护工具。

增强附加指导：维护工具包括，如：用于指导信息系统维护的诊断和测试设备。

(2) 应在所有介质在信息系统中使用前，组织应检查所有包含恶意代码诊断测试程序的介质。

(3) 组织检查所有具有保存信息功能的维护设备，以确保组织信息没有被写入设备中，或在设备发布前适当的清理设备；如果设备不能被清理，设备应保留在设施内或被破坏掉，除非有适当的组织官员明确的批准一个特例。

ICS增强附加指导：在某些情况下，组织认为实施自动机制是不合适或者不可取的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

(4) 组织使用自动化的机制限制仅有授权人员方可使用维护工具。

LOW Not Selected	MOD MA-3	HIGH MA-3 (1) (2) (3)

MA-4 远程维护

控制：组织批准、监测、并控制任何投入使用的远程可执行维护和诊断行为。

附加指导：个体可以通过外部非组织控制的网络（如Internet）指导远程维护和诊断操作。对远程维护和诊断工具的使用必须与信息系统中的组织策略和归档的安全计划保持一致。组织保存了所有远程维护和诊断操作的记录。其他为了改进远程维护安全的技术和控制包括：（i）关于通讯的加密和解密；（ii）强鉴别和认证技术，如NIST SP 800-63中描述的等级3或4标记。（iii）远程无连接确认。当远程维护完成时，组织（有时候可能是信息系统）决定在操作执行中终止所有的会话和远程连接。如果使用基于口令认证来完成远程维护，组织将在每次远程维护服务后更改口令。NIST SP 800-88提供了介质消禁方面的指导建议。NSA在网站 *http://www.nsa.gov/ia/government/mdg.cfm*上提供了一份关于已批准的介质消禁产品列表。相关安全控制：IA-2，MP-6。

增强控制：

(1) 组织审核所有的远程维护和诊断会话，并由适当的组织个人回顾远程会话的维护记录。

(2) 组织在信息系统安全策略中标明远程维护和诊断的安装和使用链接。

(3) 组织不允许远程维护或诊断服务由一个提供商执行，而且该提供商还不在自己的信息系统上实施与执行该服务的系统上一样高的安全等级。除非在服务开始之前被维护的部分从信息系统中移除并消禁了（关于组织信息）并且在服务执行之后连接到信息系统之前也消禁了（关于潜在的恶意软件）。

ICS增强附加指导：在某些情况下，组织认为实施措施加强（3）是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

LOW MA-4	MOD MA-4	HIGH MA-4 (1) (2) (3)

MA-5 维护人员

控制：组织只允许授权个体执行信息系统上的维护操作。

附加指导：当维护操作允许访问组织信息或者将导致未来机密性，完整性，可用性的妥协时，维护人员（无论是负责本地维护还是远程维护）有对信息系统的适当访问权限。当维护人员没有获得必要的访问权限时，有适当访问权限的组织人员监督维护人员在信息系统上执行的维护行为。

增强控制：无。

LOW MA-5	MOD MA-5	HIGH MA-5

MA-6 及时维护

控制：在[指定：由组织自定义的一段时间周期]的失败中，组织将获得维护支持和一些[指定：由组织自定义的关键信息系统部件列表中]的备用部件。

附加指导：无。

增强控制：无。

LOW Not Selected	MOD MA-6	HIGH MA-6

类： 介质保护(MP)
CLASS：OPERATIONAL

MP-1 介质保护策略和章程

控制：组织开发、发布、定期检查/升级：(i)一个正式的存档的介质保护策略，其标明了目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及顺从关系。(ii)正式的存档的章程，用来促进介质保护策略和相关介质保护控制的执行。

附加指导：介质保护策略和章程要与可适用的联邦法律、指示、策略、规则、标准及向导相一致。介质保护策略可以包含在组织的通用信息安全策略中，作为其一部分。需要时，可以为一般的安全程序或特殊信息系统制定应急计划章程。NIST特别报告800-12提供了安全策略和章程的指导建议。

增强控制：无。

LOW MP-1	MOD MP-1	HIGH MP-1

MP-2 介质访问

控制：组织确保只有授权的用户才能访问信息系统中的介质。

附加指导：信息系统的介质包括数字介质（如磁盘，磁带，外部的/可移动硬盘，闪盘，压缩盘，数字视频盘）和非数字介质（如纸，胶卷）。该控制也适用于具有信息存储功能的便携式和移动的计算通讯设备（如笔记本电脑，个人数字助理，移动电话）。

一份组织风险评估报告可以指导介质和相关信息容器的选择，对那些介质的访问需要严格的访问控制。组织为策略和章程建立文档，对介质的访问需要严格控制，个体授权访问介质，并且使用明确的规则来严格控制访问。该控制使用的严格控制与介质中包含的FIPS199信息的安全分类相称。例如，对那些（其包含的信息是有组织决定的，属于公共范围或公开发布的，或即使被非授权个体访问，对组织或个人产生有限影响或几乎没有影响的）介质，则需要更少的保护措施。这些情况下，我们认为对介质所在的设备的物理访问控制提供了足够的保护。

增强控制：

(1) 组织使用自动化机制来限制对介质存储区域的访问并审核尝试的访问和授权的访问。

附加增强指导：该控制增强主要用于组织（该组织存储了大量的介质）内指定的介质存储区域，但并不准备用于存储介质的任何地方（如个人办公室）。

LOW MP-2	MOD MP-2(1)	HIGH MP-2 (1)

MP-3 介质标签

控制：组织:(i)将外部标签粘贴到可移动的信息储存介质和信息系统输出上，标记信息的分配限制和处理警告以及可适用的安全标记。（ii）从标记中免除[指定：组织自定义的关于介质类型或硬件部件的列表]，只要他们仍存在于[指定：组织自定义的保护环境]中。

附加指导：组织的风险评估报告为需要标签的介质的选择提供指导。组织以策略和章程的形式建立文档，指明需要物理保护的介质以及承担此类保护所需要采取的明确措施。该控制使用的严格性与介质中包含的FIPS199信息的安全分类相当。例如，标签对那些（其包含的信息是有组织决定的，属于公共范围或公开发布的）介质并不是必须的。

增强控制：无。

LOW Not Selected	MOD MP-3	HIGH MP-3

MP-4 介质储存

控制： 组织在可控制区域内物理地控制和安全地存储信息系统介质。

附加指导：信息系统的介质包括数字介质（如磁盘，磁带，外部的/可移动硬盘，闪盘，压缩盘，数字视频盘）和非数字介质（如纸，胶卷）。可控制区域是任何区域或空间，组织信任由该空间提供的物理和程序上的保护足以满足为保护该信息或信息系统而建立的要求。该控制也适用于具有信息存储功能的便携式和移动的计算通讯设备（如笔记本电脑，个人数字助理，移动电话）。电话系统也被认为是信息系统并且具备在内部介质（如语音邮件系统）上存储信息的能力。由于在大多数情况下，电话系统没有鉴别，认证和访问控制机制（这些机制代表性地应用与其他的信息系统中），所以组织人员对电话语音邮件系统中存储的信息格外小心。

组织的风险评估报告为需要物理保护的介质以及介质上包含的相关信息的选择提供指导。组织以策略和章程的形式建立文档，指明需要物理保护的介质以及承担此类保护所需要采取的明确措施。该控制使用的严格性与介质中包含的FIPS199信息的安全分类相当。例如，对那些（其包含的信息是有组织决定的，属于公共范围或公开发布的，或即使被非授权个体访问，对组织或个人产生有限影响或几乎没有影响的）介质，则需要更少的保护措施。这些情况下，我们认为对介质所在的设备的物理访问控制提供了足够的保护。组织保护有组织标记的信息系统介质，直到介质被破坏或使用已批准的设备，技术和程序清洁过了。

作为深度防御保护战略的一部分，组织认为应该对选择的二级存储设备上按计划对静止的信息进行加密。FIPS199安全分类提供了选择二级存储加密的指导建议。组织实施有效的密钥管理来支持二级存储加密提供保护以使得在用户丢失密钥的情况下仍然能获得信息。NIST SP 800-56和800-57提供了关于密钥产生和密钥管理方面的指导建议。相关安全控制：CP-9, RA-2.

增强控制：无。

LOW Not Selected	MOD MP-4	HIGH MP-4

MP-5 介质传输

控制：组织在可控制区域以外的传输期间保护和控制信息系统介质，并限制授权个体与该介质传输有关的操作。

附加指导：信息系统的介质包括数字介质（如磁盘，磁带，外部的/可移动硬盘，闪盘，压缩盘，数字视频盘）和非数字介质（如纸，胶卷）。可控制区域是任何区域或空间，组织信任由该空间提供的物理和程序上的保护足以满足为保护该信息或信息系统而建立的要求。该控制也适用于具有信息存储功能的便携式和移动的计算通讯设备（如笔记本电脑，个人数字助理，移动电话），这些设备都是在可控制区域之外被传输的。电话系统也被认为是信息系统并且具备在内部介质（如语音邮件系统）上存储信息的能力。由于在大多数情况下，电话系统没有鉴别，认证和访问控制机制（这些机制代表性地应用与其他的信息系统中），所以组织人员极度谨慎地对待电话语音邮件系统（这些系统也是在可控制区域之外被传输的）中存储的信息类型。组织的风险评估报告为需要物理保护的介质以及介质上包含的相关信息的选择提供指导。组织以策略和章程的形式建立文档，指明在传输过程中需要保护的介质以及保护此类传输介质所需要采取的明确措施。该控制使用的严格性与介质中包含的FIPS199信息的安全分类相当。组织的风险评估报告也对运输非数字介质时选择和使用适当存储容器提供了指导建议。授权运输和快递人员可以包括组织以外的个体（如美国邮政服务或商业运输或传递服务）。

增强控制：

(1) 在可控制区域以外的传输过程中，组织使用其自定义的安全措施（如上锁的容器，加密系统）来保护数字和非数字的介质 。

附加增强控制：根据FIPS199驻留在介质上的信息的安全分类标准，以及生效的法律，可执行命令，指令，策略，规则，标准和指导，组织批准了保护数字和非数字介质的物理和技术的安全措施。加密机制可以根据使用的机制提供机密性和完整性保护。

(2)组织使用其自定义的记录系统来记载适当的，与信息系统介质运输相关的信息。

附加增强控制 ：组织按照风险评估报告，为与信息系统介质运输相关的操作建立文件需求。

(3) 组织长期雇佣一名管理员来运输信息系统介质。

附加增强控制：组织按照风险评估报告，为与信息系统介质运输相关的操作建立文件需求。

LOW Not Selected	MOD MP-5(1)(2)	HIGH MP-5(1)(2)(3)

MP-6 介质消禁与处置

控制: 在为再次使用而处理或发布之前，组织将消禁数字和非数字的信息系统介质。

附加指导: 消禁是一个用来将信息从信息系统介质上移除的过程，并且这些信息不能被回收或重建，因此为信息的机密性提供合理的保证。清理技术包括清除，净化，以及破坏介质信息,防止组织信息对非授权个体的泄露(当该介质被回收或丢弃时)。组织在包含下列信息的介质上对清理技术和流程进行判断，这些信息包括: 处在公共区域的或公开发布的信息，或对组织或个体没有负面影响（即使被回收或丢弃）的信息。NIST SP 800-88提供了关于清理方面的指导建议。国际安全代理也在网站*http://www.nsa.gov/ia/government/mdg.cfm*上提出了介质清理指导以及被批准的清理产品列表。

增强控制:

(1) 组织追踪，证明并检验介质清理行为。

(2) 组织定期地检测清理设备和流程以确保其能正确的执行任务。

LOW MP-6	MOD MP-6	HIGH MP-6(1)(2)

类： 物理和环境保护(PE)
CLASS： OPERATIONAL

PE-1 物理和环境保护的策略和流程

控制：组织开发、发布和定期检查/升级：(i)一个正式的归档的物理和环境保护策略，其标明了目的、范围、角色、责任、管理承诺、组织实体之间的协调关系以及顺从关系。(ii)正式的存档的章程，用来促进物理和环境保护策略和相关物理和环境保护控制的执行。

附加指导：物理和环境保护策略和流程同可适用的联邦法律、可执行命令，指令、策略、规则、标准及向导相一致。物理和环境保护策略可以包含在组织的通用信息安全策略中，作为其一部分。需要时，可以为一般的安全程序或特殊信息系统制定应急计划章程。NIST特别报告800-12提供了安全策略和章程的指导建议。

增强控制：无。

LOW PE-1	MOD PE-1	HIGH PE-1

PE-2 物理访问权限

控制：组织开发并保存当前对信息系统所在设备（除了那些官方指定的设备内的公共访问区域）的具有访问权限的人员的列表，并发布适当的授权证书。组织内的指派官员[指定：在组织自定义的时间周期内，至少一年一次]检查并批准访问列表和授权证书。

附加指导：适当的授权证书包括，例如徽章，标记卡和智能卡。组织迅速地将那些不再需要访问信息系统所在设备的人员从访问列表中移除出去。

增强控制：无。

LOW PE-2	MOD PE-2	HIGH PE-2

PE-3 物理访问控制

控制：组织控制了信息系统所在的（除了那些官方指定的设备内的公共访问区域）设备的所有物理访问结点（包括指定的进入/退出结点），并在准许个体对设施的访问前检验其访问授权。按照组织的风险评估报告，组织也控制对适当的公共指定区域的访问。

附加指导：组织使用物理访问设备（例如，钥匙、密码锁、暗码、读卡机）和/或配备门卫以控制人员进入包含信息系统的设施。组织按规则保护钥匙、密码锁和其他访问控制设备，并存盘这些设备的详细目录。组织更换密码锁和钥匙：(i) 定期性的；(ii) 当钥匙丢失了，密码锁被泄露了，或人员被调动或离职了。工作站和连接到组

织信息系统的外围设备可能被置于公共指定区域内，并适当控制了该区域内对这些设备的访问。若使用联邦个人身份确认证书（PIV）作为一种鉴别标记和基于标记的访问控制，访问控制系统将遵守FIPS201和NIST SP 800-73中的要求。如果基于标记的访问控制函数使用加密算法验证的话，访问控制系统将遵守NIST SP 800-78中的要求。如果基于标记的访问控制功能使用生物特征验证的话，访问控制系统将遵守NIST SP 800-76中的要求。

增强控制:

(1) 组织控制对信息系统的物理访问，这些控制独立于对设施的物理访问控制。

附加增强控制：一般来说，该增强控制适用于服务器空间，通讯中心，或其他任何设备（该设备高度集中了信息系统组件或具有比大多数设备更高影响等级的组件）内的区域。目的是为组织中更易受攻击的的区域提供物理安全附加层（这些区域之所以更易受攻击，是因为它们大量集中了信息系统组件或那些具有高影响等级的组件）。该增强控制并不适用于那些分散的，人员日常使用的工作站或外围设备。

LOW PE-3	MOD PE-3	HIGH PE-3

PE-4 传输介质的访问控制

控制：组织控制对信息系统分布以及组织设施内传输线路的物理访问。

附加指导：应用于信息系统分布和传输线路的物理保护措施有助于阻止意外破坏，崩溃，和物理损害。并且，物理保护措施有必要用于帮助防止窃听或非加密数据传输过程中的篡改。用于控制对信息系统分布和传输线路的保护措施包括：（i）上锁的配线室；（i）无连接的或上锁的备用插座；（iii）通过导线管或电缆桥架来保护电缆。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

PE-5 显示介质的访问控制

控制：组织控制对信息系统设备的物理访问，这些设备显示信息以阻止未授权的个体观察显示输出。

附加指导：无。

增强控制：无。

LOW Not Selected	MOD PE-5	HIGH PE-5

PE-6 物理访问的监控

控制：组织监控对信息系统的物理访问，以侦测并响应物理安全事件。

附加指导：组织定期回顾物理访问日志，调查明显的安全侵害或可疑的物理访问行为。对检测到的物理安全事件做出响应，是组织事件响应能力的一部分。

增强控制：

(1) 组织集中监控实时入侵警报和监视装置。

(2) 组织使用自动化的机制确保能识别潜在的入侵并发起适当的响应行为。

LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (2)

PE-7 访客控制

控制：组织通过如下方式控制对信息系统的物理访问：在授权访问设备（信息系统驻留在该设备中，而不是那些被指定为公共访问的区域中）之前对访问者进行认证。

附加指导：政府官员和那些有永久信任证书的人不属于这里所说的访客。联邦雇员和承包人的个人身份检验证书遵守FIPS201，根据NIST特别版800-79的规定，PIV证书的发布组织也是被认可的。

增强控制：

(1) 当需要时组织陪同并监视访客的行为。

LOW PE-7	MOD PE-7 (1)	HIGH PE-7 (1)

PE-8 访问日志

控制：组织保存访客访问设备（信息系统驻留在该设备中，而不是那些被指定为公共访问的区域中）的日志，它包括：(i) 来访人员的名字和所属组织；(ii)访客的签名；(iii)鉴别形式；(iv)访问的数据；(v)进入和离开的时间；(vi)访问的目的；(vii)被访问人员的名字和所属组织。组织中指派官员按组织自定义的时间周期检查访问日志。

附加指导：无。

增强控制：

(1) 组织使用自动化的机制促进访问日志的维护和回顾。

(2) 组织维护所有物理访问的记录，包括访客和授权用户。

LOW PE-8	MOD PE-8 (1)	HIGH PE-8 (1)

PE-9 电力设备和电缆

控制：组织保护用于信息系统的电力设备和电缆，避免损伤或毁坏。

附加指导：无。

增强控制：

(1) 组织使用冗余的平行的电缆线路。

LOW Not Selected	MOD PE-9	HIGH PE-9

PE-10 紧急断电

控制：组织为设备（这些设备中高度集中了信息系统的资源）内的特别场所提供断电功能。该功能是针对那些即使不允许危险分子接近，该设备也可能会故障或受到威胁的信息系统组件。

附加指导：高度集中了信息系统资源的设备包括，例如，数据中心，服务器房以及主机房。

增强控制：

(1) 组织保护紧急断电功能，以避开意外操作和非授权操作。

LOW Not Selected	MOD PE-10	HIGH PE-10 (1)

PE-11 紧急备用电源

控制：组织提供一个短期的不间断电力供应，以便信息系统在主电源丧失事故中能有序的关闭。

附加指导：无。

增强控制：

(1) 组织提供给信息系统一个长期备用的电力供应系统，该信息系统能够在主电源长期丧失的事故中有能力维持信息系统所必须的最小的运行能力。

(2) 组织提供给信息系统一个长期的备用电力供应系统，该信息系统是独立运行而不依赖外部电源的。

LOW Not Selected	MOD PE-11	HIGH PE-11 (1)

PE-12 紧急照明

控制：组织使用和维护紧急照明系统，该系统在电力损耗或中断事故中被激活，并包括紧急出口和逃离通道。

附加指导：无。

增强控制：无。

LOW PE-12	MOD PE-12	HIGH PE-12

PE-13 防火

控制：组织使用和维护防火灭火设备/系统，并在火灾事故中启用它们。

附加指导：防火灭火设备/系统包括但不限于洒水系统、手动灭火器、固定灭火水龙带和冒烟检测设备。

增强控制：

(1) 组织使用防火设备/系统，该设备/系统在火灾事故中会自动激活并通知组织和紧急事件处理员。

(2) 组织使用灭火设备/系统，该设备/系统为组织和紧急事件处理员提供任何激活操作的自动通知。

(3) 组织在设备（这些设备并不是长期使用的）中使用自动灭火功能。

LOW PE-13	MOD PE-13 (1)(2)(3)	HIGH PE-13 (1) (2) (3)

PE-14 温度和湿度控制

控制：组织在可接受的等级内规范地维护并监控信息系统所在设备的温度和湿度。

附加指导：无。

增强控制：无。

LOW PE-14	MOD PE-14	HIGH PE-14

PE-15 防水

控制：组织提供易用的，能正确工作的，并为关键人员所熟悉的主关闭阀，以保护信息系统免受由水管断掉或其他漏水源而造成的水破坏。

附加指导：无。

增强控制:

(1) 组织使用不需要人工干涉的自动化机制，使得在重大的漏水事故中能保护信息系统免受水灾。

LOW PE-15	MOD PE-15	HIGH PE-15 (1)

PE-16 传输和移除

控制: 组织授权并控制信息系统相关项目进入和离开设施，并维护这些项目的适当记录。

附加指导: 组织控制传输区域，如果可能的话，从信息系统和介质库中孤立这些区域以防止未授权的访问。

增强控制: 无。

LOW PE-16	MOD PE-16	HIGH PE-16

PE-17 备用工作场所

控制: 组织在备用工作场所中使用适当的管理，以及操作的和技术的信息系统安全控制机制。

附加指导: 在发生安全问题时，组织为雇员提供了一种用来与信息系统安全人员通讯的方式。 NIST SP 800-46提供了远程交换和宽带通信中有关安全的指导。

增强控制: 无。

LOW Not Selected	MOD PE-17	HIGH PE-17

PE-18 信息系统组件的位置

控制：组织为设备内的信息系统组件分配合适的位置，用来减少由物理和环境的破坏而带来的潜在的破坏，并减少非授权访问的几率。

附加指导：物理和环境的破坏包括，例如，洪水，火灾，龙卷风，地震，飓风，恐怖活动，故意破坏，电干扰和电磁辐射。可能的时候，组织也会根据物理和环境的破坏来考虑设备的位置或地址。

增强控制：组织根据物理和环境的破坏制定信息系统所在设备的位置或地址，并针对现存设备，在缓解风险策略中考虑物理和环境破坏因素。

LOW Not Selected	MOD PE-18	HIGH PE-18(1)

PE-19 信息泄露

控制：组织保护信息系统使其免遭由电磁信号辐射造成的信息泄露。

附加指导：FIPS 199信息系统的安全章程（机密性的）和组织安全策略为安全措施和对策（这些策略和对策是用于保护信息系统使其免遭由电磁信号辐射造成的信息泄露）的使用提供了指导建议。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

类：设计/规划 (PL)
CLASS：MANAGEMENT

PL-1 安全设计/规划策略和流程

控制：组织开发、发布，并定期审查、更新：1）一个正式的归档的安全设计/规划策略，策略中定义了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）正式的存档的流程，用来帮助执行安全设计/规划策略和相关安全设计/规划控制。

附加指导：安全设计/规划策略和流程与可适用的联邦法律、可执行命令，指令、策略、规则、标准及向导相一致。安全设计/规划策略标明了有关机密性，完整性，和可用性的所有策略需求，并可以包含在组织的通用信息安全策略中，作为其一部分。可以为一般的安全程序制定安全计划章程，也可在必要时为特殊信息系统制定应急计划章程。NIST SP 800-18提供了关于安全设计/规划的指导建议。NIST SP 800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW PL-1	MOD PL-1	HIGH PL-1

PL-2 系统安全设计/规划

控制：组织为信息系统开发并执行一个信息系统安全设计/计划，在安全设计/计划中概述系统的安全要求，并描述针对这些安全要求的安全控制。组织内指定管理人员审查、批准安全设计/计划。

附加指导：安全设计/规划与组织的信息系统体系结构以及信息系统安全架构相结合。NIST SP 800-18提供关于安全设计的指导。

ICS附加指导：NIST SP 800-82为开发ICS安全计划提供了指南。

NIST SP 800-82 ICS特别推荐与指南：应当在已有IT安全项目的基础上提出ICS的安全计划。然后，ICS与IT系统的不同点导致他们具体安全实施的不同。ICS需要具有前瞻性的安全计划，以配合ICS系统持续的安全改进和抵抗新的安全威胁的能力。

增强控制：无。

LOW PL-2	MOD PL-2	HIGH PL-2

PL-3 系统安全设计/规划修正

控制：组织审查信息系统安全设计/计划[指定：组织定义的周期；至少一年一次]，，并通过修改设计/规划来标明在设计执行或安全控制评估过程中发现的系统/组织的

改变或问题。

附加指导: 组织预先定义重要的改变,并在配置管理过程中发现它们。NIST SP 800-18提供了关于安全计划/规划修改方面的指导建议。

增强控制: 无。

LOW PL-3	MOD PL-3	HIGH PL-3

PL-4 行为规范

控制: 组织针对所有信息系统用户的易用性建立一整套规范，规范中描述用户的职责以及对信息和信息系统使用的期望行为。在批准用户访问信息系统和驻留信息前，组织接收用户签署的书面确认，表示其已经读过、理解并同意遵守此行为规范。

附加指导: 用户确认行为规范可以使用电子签名（除非组织策略特别禁止）。NIST SP 800-18提供关于准备行为规范的指导。

增强控制: 无。

LOW PL-4	MOD PL-4	HIGH PL-4

PL-5 隐私影响评估

控制: 组织根据OMB政策，指导一个关于信息系统的隐私影响评估。

附加指导: OMB Memorandum 03-22(管理与预算办公室 03-22)为执行E-Government Act of 2002（2002电子政府法案）中的保密规定提供指导。

增强控制: 无。

LOW PL-5	MOD PL-5	HIGH PL-5

类：人员安全 (PS)
CLASS：OPERATIONAL

PS-1 人员安全策略和流程

控制：组织开发、发布，并定期审查、更新：1）一个正式的归档的人员安全策略，策略中定义了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）正式的存档的流程，用来帮助执行人员安全策略和相关人员安全控制。

附加指导：人员安全策略和流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、和指导。人员安全策略可以包含到组织的通用信息安全策略中作为其一部分。可以为一般的安全程序制定人员安全章程，也可在必要时为特殊信息系统制定应急人员安全章程。NIST SP800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW PS-1	MOD PS-1	HIGH PS-1

PS-2 岗位分类

控制：组织为所有岗位指定一个风险标识（risk designation），并为人员获得该职位建立筛选标准。组织在[指定：组织定义的时间周期内] 审查并修正岗位风险标识。

附加指导：岗位风险标识与5 CFR 731.106(a)、人事管理局的策略和指导是一致的。

增强控制：无。

LOW PS-2	MOD PS-2	HIGH PS-2

PS-3 人员筛选

控制：在授权访问前，组织筛选需要访问组织信息和信息系统的个人。

附加指导：筛选与以下是一致的：1）5 CFR 731.106(a)；2)人事管理局的策略、规章和指导；3）组织的策略、规章和指导；4）FIPS 201、SP800-73、SP800-76和SP800-78；5）为指定岗位风险标识而建立的标准。

增强控制：无。

LOW PS-3	MOD PS-3	HIGH PS-3

PS-4 人员离职

控制：当个人雇佣合同被终止时，组织将终止其访问信息系统、进行离职谈话，确

保所有的组织信息系统相关财产得到归还，并且给适当人员授权，使其能够访问离职人员储存在组织信息系统中的官方记录。

附加指导: 信息系统相关财产包括，例如，钥匙，标记卡，通行证。及时地执行该控制，对因故离职的雇员或定约人而言都是很重要的。

增强控制: 无。

LOW PS-4	MOD PS-4	HIGH PS-4

PS-5 人员调动

控制: 当人员再分配或调动到组织内的其他岗位时，组织审查信息系统和设备的访问权限，并执行适当的操作（例如: 重新发放钥匙、标识卡、通行证; 关闭过去的帐号、建立新的帐号; 修改信息访问权限）。

附加指导: 可能要求的适当操作包括: （i）归还旧钥匙并发放新钥匙，标记卡，通行证; （ii）关闭旧帐户并建立新帐户; （iii）更改系统访问权限; （iv）赋予访问权限，使其能访问由该职位的旧员工和旧帐户创建或控制的官方记录。

增强控制: 无。

LOW PS-5	MOD PS-5	HIGH PS-5

PS-6 访问协议

控制: 在授权访问和审查/修改协议之前，组织以[指定: 组织自定义的时间周期]为需要访问组织信息和信息系统的人员制定适当的访问协议。

附加指导: 访问协议包括，例如， 非公开协议，可接受的使用协议，行为规范以及利益冲突协议。电子签名在承认访问协议中也被接受使用，除非组织政策特别禁止。

增强控制: 无。

LOW PS-6	MOD PS-6	HIGH PS-6

PS-7 第三方人员安全

控制: 组织为第三方机构建立人员安全要求，并监控第三方提供商的符合性。

附加指导: 第三方机构包括，例如服务提供商、承包商以及其他提供信息系统开发、信息技术服务、外包应用、网络安全管理的组织。在收集的相关文档中，组织明确定义了人员安全要求。NIST SP800-35提供关于信息技术安全服务的指导。

增强控制: 无。

LOW PS-7	MOD PS-7	HIGH PS-7

PS-8 人员处罚

控制：对于没有遵守已建立的信息安全策略和流程的人员，组织采用一种正式的处罚流程。

附加指导：处罚流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、指导。处罚流程能包含到组织的通用人员策略和流程中，作为其一部分。

增强控制：无。

LOW PS-8	MOD PS-8	HIGH PS-8

类：风险评估 (RA)
CLASS：MANAGEMENT

RA-1 风险评估策略和流程

控制：组织开发、发布，并定期检查、更新：1）一个正式的归档的风险评估策略，策略中定义了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）一个正式的存档的流程，用来帮助执行风险评估策略和相关风险评估控制。

附加指导：风险评估策略和流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、指导。风险评估策略可以包含到组织的通用信息安全策略中，并作为其一部分。可以为一般的安全程序制定风险评估流程，也可在必要时为特殊信息系统制定风险评估流程。NIST SP800-30提供了关于风险评估的指导。NIST SP800-30提供了有关风险评估方面的指导；NIST SP800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW RA-1	MOD RA-1	HIGH RA-1

RA-2 安全分类

控制：组织依照可适用的联邦法律、可执行命令、指令、策略、规章、标准、指导将信息系统和由系统处理的，存储的，或传输的信息进行分类，并将该分类结果（包括支持原理）归档于信息安全计划中。组织内指派的高层管理人员审查并批准安全分类。

附加指导：FIPS199是非国际化信息和信息系统安全分类的可适用联邦标准。组织依照FIPS199 安全分类管理组织内的活动，这些活动牵涉到：首席信息官员、高级助理信息安全员、信息系统所有者、和信息所有者。根据USA2001爱国者法案和本国安全总统指示，组织也考虑对其他组织的潜在影响以及在分类信息系统方面的潜在的国家等级的影响。作为深度防御保护策略的一部分，根据组织的风险评估，组织考虑将高影响的信息系统分解成独立的物理区域（或环境）并严格限制或禁止网络访问。NIST SP800-60提供了关于确定信息系统中信息的安全分类的指导。相关安全控制：MP-4，SC-7。

ICS附加指导：NIST SP 800-82提供了ICS安全分类相关的指南。

NIST SP 800-82 ICS特别推荐与指南：作为风险框架的第一步，根据损失产生的影响对信息和信息系统进行分类。对于ICS的每种信息类型和信息系统，判断的主要根据是可用性，其次才是保密性和完整性。安全分类要和脆弱性和威胁一起用来评估组织的风险。

增强控制：无。

LOW RA-2	MOD RA-2	HIGH RA-2

RA-3 风险评估

控制：组织引导风险评估，以及对那些由对信息和信息系统的非授权访问、使用、泄露、中断、修改、破坏而造成的危害进行评估，这些信息和信息系统支持以上操作和代理资产（包括由外部团体管理/操作的信息和信息系统）。

附加指导：风险评估考虑到脆弱性、危险源、已部署的安全控制，或在适当的地方确定由组织的操作，组织的资产或基于信息系统操作的个人而引起的残留风险等级。根据USA2001爱国者法案和本国安全总统指示， 组织也考虑对其他组织的潜在影响以及在分类信息系统方面的潜在的国家等级的影响。风险评估也考虑那些由组织操作，组织资产或外部组织人员（如，服务商，代表组织的操作信息系统的定约人，访问组织信息系统的个体，外购实体）造成的风险。根据OMB政策和相关电子认证法案，可能也需要对访问联邦信息系统的公共用户进行认证以保护非公共的或私人相关的信息。同样地，组织的风险评估也指明了对联邦信息系统的公共访问。通用服务管理提供了一些工具，用来支持对联邦信息系统的公共访问处理部分的风险评估。NIST SP800-13提供了关于引导风险评估方面的指导，包括威胁，脆弱性，和影响评估。

ICS附加指导：NIST SP 800-82提供了ICS风险评估相关的指南。

NIST SP 800-82 ICS特别推荐与指南：对于ICS，风险评估最主要的一个方面就是判断从控制网络流向企业网络的数据的价值。如果由这些数据可以得出很有价值的判断，那么这些数据就很重要。最后是否采取风险降低措施取决于最后的效果和对应的花费。很多情况下，高等级的安全可以达到，但是考虑到可能的高额花费和脆弱性补救导致的功能损失，采取某些安全措施实际上是不可行的。对于ICS，风险评估更多的要考虑人员安全，健康或者产生的负面影响而不仅仅是经济因素。

增强控制：无。

LOW RA-3	MOD RA-3	HIGH RA-3

RA-4 风险评估修正

控制：组织以[指定：组织定义的周期]修正风险评估，或当信息系统、信息系统所在的设备出现重要改变，可能影响系统的安全状态或信任状态时，修正风险评估。

附加指导：组织开发并文档化那些对信息系统产生重要改变的特别标准。NIST SP800-30提供了风险评估修正的指导。

增强控制：无。

LOW RA-4	MOD RA-4	HIGH RA-4

RA-5 脆弱性扫描

控制: 组织以[指定: 组织定义的周期]扫描信息系统中的脆弱点，或当识别和报告了新的潜在地影响了系统的重要脆弱点时，进行系统脆弱性扫描。

附加指导: 组织利用适当的扫描工具和技术来扫描脆弱点。组织培训指定人员使用并维护脆弱性扫描的工具和方法。脆弱性扫描根据组织政策以及风险评估预定或随机执行。从脆弱性扫描过程中获得的信息可以被组织内的适当人员自由共享，以帮助消灭其他信息系统中相似的脆弱点。为定制软件和应用分析脆弱性时，可能需要特别的方法（例如: 适于应用软件的脆弱性扫描工具、源代码审查、源代码的静态分析）。NIST SP800-42提供了关于网络安全测试的指导。NIST SP800-40提供了关于修补及管理脆弱性的指导。

ICS附加指导: 为了保证脆弱性扫描进程不对ICS的功能产生负面影响，必须在ICS网络上小心使用扫描工具。在扫描开始之前，ICS产品可能需要离线，并且复制到可行的设备（盘区）？假如ICS必须离线评估，可以将评估安排在任何可能的计划好的ICS停机阶段。将如在非ICS网络上使用脆弱性扫描工具，一定要保证这些工具不会扫描到ICS网络。在某些情况下，组织认为实施ICS扫描是不合适的（或者产生负面影响，影响安全性，可靠性），组织应记录下使用复制系统的原理和方法。NIST SP 800-82中提供了ICS脆弱性扫描方面的指南。

NIST SP 800-82 ICS特别推荐与指南: 应该在备份的服务器或者实验室中的独立测试系统上执行脆弱性扫描。这种在实验室里面进行的脆弱性扫描可以显示出会对操作系统造成的损害。即使通过良好的配置管理保证实验室中的测试具有很高的代表性，在对实际系统进行操作时也可能会出现问题。

增强控制:

1）组织使用脆弱性扫描工具，这些工具具有易于更新信息系统中已扫描到的脆弱性列表的功能。

2）组织以[指定: 组织定义的周期]，或当重要的新的脆弱性被识别和报告时，更新信息系统中已扫描到的脆弱性列表。

3）组织使用脆弱性扫描流程，该流程示范了扫描范围的宽度和深度，包括脆弱性检查以及信息系统部件扫描。

LOW Not Selected	MOD RA-5	HIGH RA-5 (1) (2)

类： 系统与服务采购(SA)
CLASS：MANAGEMENT

SA-1 系统与服务采购策略与流程

组织开发、发布，并定期检查、更新：1）一个正式的归档的系统与服务采购策略，策略中包括信息安全事项并定义了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）一个正式的存档的流程，用来帮助执行系统与服务采购策略和系统与服务采购相关的控制措施。

附加指导：系统与服务采购策略和流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、指导。系统与服务采购策略可以包含到组织的通用信息安全策略中，并作为其一部分。可以为一般的安全程序制定系统与服务采购流程，也可在必要时为特殊信息系统制定系统与服务采购流程。NIST SP800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW SA-1	MOD SA-1	HIGH SA-1

SA-2 资源分配

控制：作为资金规划和投资控制过程的内容之一，组织应决定、证明和分配保护信息系统所需要的足够资源。

附加指导：组织在任务/作业计划中定义信息系统的安全需求，并且在组织的规划和预算文件中为信息系统安全立项。NIST SP 800-65提供了将安全内容集成到资金计划和投资控制程序的指南。

增强控制：无。

LOW SA-2	MOD SA-2	HIGH SA-2

SA-3 生命周期支持

控制：组织采用系统开发生命周期方法论管理信息系统，该方法论中包括信息安全相关内容。

附加指导：NIST SP 800-64提供了关于系统开发生命周期中的安全事项的指导。

增强控制：无。

LOW SA-3	MOD SA-3	HIGH SA-3

SA-4 采购

控制: 组织将基于风险评估确定的安全需求和/或安全规范，不论是明确说明的或被提及的内容都包含到信息系统采购合同文档中，并与可适用的法律、可执行命令、指令、策略、规章、标准、指导相一致。

附加指导:

引出的文档

为信息系统和服务所引出的文档（例如：建议请求），不论明确的或被提及的内容，都包括描述如下问题的安全要求：(i)要求的安全能力（安全需要和必要时详细的安全控制及其他详细的FISMA要求）；(ii) 要求的设计和开发方法；(iii)要求的测时和评估流程；(iv)要求的文档。当新的威胁/脆弱性被识别，或者新的技术被应用时，应当对这些引出文档中的要求进行更新。NIST SP 800-36中提供了选择信息安全产品的指导。NIST SP 800-35提供了有关信息技术安全服务方面的指导。NIST SP 800-64提供了对系统开发生命周期中的安全事项的指导。

信息系统文件

引出文件包括对适当信息系统文件的需求。该文件中包含用户和系统管理员指南和如何执行信息系统安全控制方面的信息。文档的详细程度是根据FIPS199信息系统安全分类来定的。

测试、评估与验证产品

NIST SP 800-23提供了关于采购和使用已通过测试和评估的信息技术产品的指南。

配置设置和执行指导

信息系统所必需的文档包括安全配置设置和安全实施指南。OMB FISMA报告指导中提供了联邦信息系统配置需求方面的指导。NIST SP 800-70提供了信息技术产品配置设置方面的指南。

ICS附加指导: SCADA与ICS获取项目提供了一系列普通的ICS获取语言(???)。*http://www.msisac.org/scada/*。

增强控制:

(1) 组织要求在采购文档中应包含描述信息系统安全控制措施的功能特性的文档，并具有足够的细节便于控制措施的分析和测试。

(2) 组织要求在采购文档中应包含描述信息系统安全控制措施的设计和实施的细节，并具有足够的描述便于控制措施的分析和测试。（包括控制部件之间的功能接口）。

LOW SA-4	MOD SA-4(1)	HIGH SA-4 (1)

SA-5 信息系统文档

控制: 组织按照要求获取并保护足够的信息系统文档，并使授权人员可以访问这些文档。

附加指导: 文档包括管理员和用户有关以下几方面的指导信息: (i)信息系统的配置、安装和操作; (ii)有效的使用信息安全特征。当适当的信息系统文档不可用或不存在时（如，由于系统老化或缺乏商家/厂商的支持），组织文档应包括此类文档并在需要时提供修补偿安全控制 。

增强控制:

(1) 除了管理和用户指南，如果可能的话，组织应从厂商和生产商那里获取描述安全措施功能特性的文档，并具有足够的细节便于控制措施的分析和测试。

(2) 除了管理和用户指南，如果可能的话，组织应从厂商和生产商那里获取描述安全措施设计与实施的文档，并具有足够的细节便于控制措施（包括控制组件间的功能接口）的分析和测试。

LOW SA-5	MOD SA-5 (1)	HIGH SA-5 (1) (2)

SA-6 软件使用限制

控制: 组织遵守软件使用限制。

附加指导: 按照合同条款和法律权力使用软件和相关文档。对那些受产权保护的软件和相关文档，组织使用跟踪系统来控制拷贝和分发。组织控制并记录端到端文件存取共享技术的使用情况，以确保这些技术不被用来对受版权保护的产品进行未授权的分发、显示、执行和复制。

增强控制: 无。

LOW SA-6	MOD SA-6	HIGH SA-6

SA-7 用户软件安装

控制: 组织执行明确的规章管理用户对软件的安装。

附加指导: 如果提供了授权，用户就能够安装软件。组织鉴别哪些软件类型是允许安装的（例如: 对现有软件进行升级和打安全补丁的程序），并且确定哪些软件类型是禁止安装的（例如: 仅限于个人使用的免费软件，非政府机构使用的，以及一些背景不清楚或可疑的暗藏恶意代码的软件）。

增强控制: 无。

LOW SA-7	MOD SA-7	HIGH SA-7

SA-8 安全性设计原则

控制：采用安全工程原则设计和实现信息系统。

附加指导：NIST SP 800-27中提供了对信息系统安全性工程原则的指南。安全工程原理主要应用于新开发的信息系统或正在进行重要升级的系统，并被整合到系统开发生命周期中。对遗留下来的信息系统，组织尽量将安全工程原理应用于系统升级和修改中，并给出系统中硬件，软件和防火墙组件的当前状态。

ICS附加指导：NIST SP 800-82中提供了ICS深度防御保护策略的相关指南。

NIST SP 800-82 ICS特别推荐与指南：DHS的控制系统安全计划策略的主要内容是在ICS架构中使用防火墙，DMZ和IDS。通过使用多个DMZ可以将功能模块分离出来，实现对具有不同操作功能的大规模网络的保护。而且可以在不用的网络域中应用不同规则和签名的入侵检测。

增强控制：无。

LOW Not Selected	MOD SA-8	HIGH SA-8

SA-9 外部信息系统服务

控制： 组织：（i）要求外部信息系统服务的提供商使用适当的安全控制，与可适用的法律、可执行命令、指令、策略、规章、标准、指导和已建立的服务等级协议相一致。（ii）监督安全控制的一致性。

附加指导：外部信息系统服务是在组织信息系统可信赖边界之外执行的服务（如，由组织信息系统使用，但不包括在信息系统之中的服务）。与外部服务提供商之间的关系通过各种各样的方式来建立，例如，合资企业，商业伙伴，外包约定（如，通过合约，内部代理协议，一系列的商业约定），专利使用权转让协议，供应链协作平台。最终，由于使用外部信息系统而带来的关于减轻组织操作和资产以及个人的风险方面的责任应当由授权官员来承担。当处理许多与信息系统安全相关的问题时，授权官员必须要求与外部服务商建立一条信用链。对于组织外部的服务而言，信任链要求组织建立并保持一种信任等级，以使得在这种潜在的复杂的消费者-供应商关系中每个参与服务的供应商，能为向组织提供的服务提供适当的保护。当不能在外部服务或服务提供商之间建立足够可信的等级时，组织使用补偿安全控制并/或接受对组织的操作和资产，或对个体的更高层次的风险。外部信息系统服务文档中包括政府，服务提供商，最终用户安全任务和责任，以及任何安全等级的协议。安全等级的协议为每个要求的控制定义期望的操作，描述可量化的输出，为任何不一致的情况指明补救措施和响应要求。NIST SP800-38提供了关于信息技术安全服务方面的指导。NIST SP800-64提供了关于系统开发生命周期中安全事项的指导建议。

增强控制：无。

LOW SA-9	MOD SA-9	HIGH SA-9

SA-10 开发者配置管理

控制：组织要求信息系统开发者创建并执行一套配置管理计划，该计划控制系统在开发过程中的变更，跟踪安全漏洞，请求变更授权，并提供计划和执行文档。

附加指导：该控制也适用于与信息系统变更有关的开发活动。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH SA-10

SA-11 开发者安全测试

控制：组织要求信息系统开发者创建一套安全测试和评估计划，执行该计划，并归档其结果。

附加指导：当开发过程中的安全测试结果被验证，并认可开发测试后对信息系统的安全修改将会对这些结果产生影响之后，开发安全测试结果将被最大程度的使用。测试结果将被用于支持运输信息系统时的安全鉴别和授权过程。相关安全控制：CA-2，CA-4。

ICS附加指导：总的来说，试验性的安全测试不应该在ICS上执行，试验性的安全测试不应对ICS的正常运行产生不良影响。

增强控制：无。

LOW Not Selected	MOD SA-11	HIGH SA-11

类： 系统与通信保护(SC)
CLASS：TECHNICAL

SC-1 系统与通信保护策略与流程

控制：组织开发、发布，并定期检查、更新：1）一个正式的归档的系统与通信保护策略，策略中标明了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）一个正式的存档的流程，用来帮助执行系统与通信保护策略和系统与通信保护相关的控制。

附加指导：系统与通信保护策略和流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、指导。系统与通信保护策略可以包含到组织的通用信息安全策略中，并作为其一部分。可以为一般的安全程序制定系统与通信保护流程，也可在必要时为特殊信息系统制定系统与通信保护流程。NIST SP800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW SC-1	MOD SC-1	HIGH SC-1

SC-2 应用划分

控制：信息系统把用户功能（包括用户接口服务）从信息系统管理功能中划分出来。

附加指导：信息系统把用户接口服务（例如：公开Web页）在物理和逻辑上从信息存储和管理服务（例如：数据库管理）中划分出来。该划分可以通过使用不同的计算机、不同的中央处理单元、不同的操作系统实例、不同的网络地址，以及这些方法的混合，或其他恰当的方法来实现。

增强控制：无。

LOW Not Selected	MOD SC-2	HIGH SC-2

SC-3 安全功能隔离

控制：信息系统将安全功能和非安全功能进行隔离。

附加指导：信息系统通过磁盘分区、域划分等方法将安全功能从非安全功能中隔离出来，包括：访问控制，硬件、软件以及执行安全功能的平台固件的完整性等内容。信息系统为每个执行的进程维护隔离执行的域（例如：地址空间）。

ICS附加指导：在某些情况下，组织认为实施措施或措施加强是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制:

(1) 信息系统采用低层硬件划分机制来促进安全功能隔离。

(2) 信息系统从非安全功能和其他安全功能中隔离出重要的安全功能（例如：强制访问和信息流控制功能）。

(3) 信息系统将包括在含有安全功能的隔离边界内的非安全功能的数量最小化。

(4) 信息系统安全功能以大规模的独立模块形式实现，这些独立的模块可以避免模块间不必要的交互。

(5) 信息系统安全功能以分层的结构来实现，减小了设计层之间的交互，并避免了底层对高层的功能性或正确性的依赖。

LOW Not Selected	MOD Not Selected	HIGH SC-3

SC-4 信息残余

控制：信息系统通过系统资源共享的方式阻止未授权和无意识的信息传输。

附加指导：当当前用户/角色（当前进程）能够访问共享包含之前用户产生的信息的系统资源（如注册表、内存、第二存储器），信息系统残余控制（有时称为对象重用，或数据残留），阻止任何当前用户/角色（当前进程）使用访问由之前的用户/角色的操作（或代表之前用户进程的操作）产生的信息，包括加密信息。

增强控制：无。

LOW Not Selected	MOD SC-4	HIGH SC-4

SC-5 拒绝服务保护

控制：信息系统保护或限制由以下类型的拒绝服务攻击造成的影响：[指定：组织定义的拒绝服务攻击列表或当前列表的参考源]。

附加指导：存在一些用来限制或有时候可以消除拒绝服务攻击的影响的技术。例如，边界保护设备可以过滤特定类型的包以保护组织内部网络的设备被拒绝服务攻击直接影响。使用增加的容量和带宽并结合服务冗余技术可保护那些公共访问的信息系统。

增强控制:

（1） 信息系统严格限制用户对其他信息系统或网络发起拒绝服务攻击的能力。

（2） 信息系统管理多余的容量，带宽或其他冗余来限制拒绝服务攻击的信息流类型所带来的影响。

LOW SC-5	MOD SC-5	HIGH SC-5

SC-6 资源优先级

控制：信息系统通过优先级限制对资源的使用。

附加指导：优先级保护策略确保低优先级的进程不能延迟或干涉任何为高优先级进程服务的信息系统。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

SC-7 边界保护

控制：信息系统监视并控制在信息系统外部边界和系统中的关键内部边界上的通信。

附加指导：任何与Internet、其他的外部网络或信息系统的连接必须经过包含适当边界保护设备（例如：代理服务器、网关、路由器、防火墙、加密通道等）的管理接口来实现的，这些边界保护设备被安放在有效的体系结构中（如路由器，它是用来保护防火墙以及驻留在受保护子网中的应用网关，该子网通常称为DMZ）。边界保护机制的运行故障不应导致任何未授权的、在信息系统边界外的信息发布。任何指定交互处理点的信息系统边界保护都提供与关键点一样的保护水平。

作为深度保护策略的一部分，组织考虑将高影响的信息系统分解为几个独立的物理区域（或环境）并根据组织的风险评估报告，将上述可管理接口的概念用于限制或禁止网络访问。FIPS199安全分类为适当的域划分候选方案的选择提供指导。

在执行与使用此类服务相关的安全控制时，组织应慎重考虑商业通讯服务所固有的共享本性。商业通讯服务通常都是基于网络组件和被所有附带的商业顾客所共享的加固管理系统，可能包括提供访问路线和其他服务元素的第三方。因此，尽管提供了安全防备，互接传输服务也可能成为增加的风险源。因此，当此类状况发生时，组织要么执行相应的补偿安全控制，要么明确地接受附加的风险。NIST SP800-77提供了关于VPN的指导。相关安全控制：MP-4，RA-2。

增强控制：

（1） 组织从物理上将可公开访问的信息系统组件划分到具有独立物理网络接口的独立子网中。除非有适当的网关保护，否则不允许外部公众访问进入组织内部网络。

附加增强指导：公开访问的信息系统组件包括：如，公开的web服务器。

ICS附加增强指导：总的来说，ICS信息不应该发布在公共场合。

（2） 组织阻止对内部网络的公开访问，除非经过适当的中介。

（3） 组织限制信息系统的访问点的数量，以便更好地监视边界内外的网络流量。

（4） 组织使用一种具有任何外部通讯服务的可管理的接口（一种采用有效的安全体系结构的边界保护设备），来实施适合于被传输信息的机密性和完整性要求的保护控制措施。

（5） 信息系统拒绝那些由默认带来的网络流量，允许那些由例外带来的网络流量（如，拒绝所有，特别准许）。

（6） 组织阻止信息系统边界外部未授权的信息发布，或当边界保护机制的操作失败时，组织将阻止那些通过信息系统边界的未授权的通信。

LOW SC-7	MOD SC-7 (1) (2)(3)(4)(5)	HIGH SC-7 (1) (2) (3) (4) (5) (6)

SC-8 传输完整性

控制：信息系统保护传输信息的完整性。

附加指导：如果组织对传输服务的商业服务提供商的依赖，是一种日常行为而非完全的专注服务的话，获得必要保证将更加困难，该保证与传输完整性所需要的安全控制的执行有关。当不可能通过适当的契约手段获得必要的安全控制并保证控制有效性时，组织要么执行适当的补偿安全控制，要么明确地接受附加的风险。NIST SP800-52提供了关于使用传输层安全（TLS）来保护传输完整性的指导。NIST SP800-77提供了关于使用IPsec来保护传输完整性的指导。NIST SP800-81提供了关于域名系统（DNS）消息认证和完整性鉴别的指导。NSTISSI No.7003包含了使用保护性分布式系统的指导。

增强控制：

(1) 组织使用加密机制来识别传输过程中对信息的更改，除非受到另外的可选择的物理措施的保护。

附加增强指导：可选择的物理保护措施包括，例如，保护性的分布式系统。

ICS附加增强指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。相关的安全措施；PE-4,SC-13。

LOW Not Selected	MOD SC-8	HIGH SC-8 (1)

SC-9 传输机密性

控制： 信息系统保护传输信息的机密性。

附加指导：如果组织对传输服务的商业服务提供商的依赖，是一种日常行为而非完

全的专注服务的话，获得必要保证将更加困难，该保证与传输机密性所需要的安全控制的执行有关。当不可能通过适当的契约手段获得必要的安全控制并保证控制有效性时，组织要么执行适当的补偿安全控制，要么明确地接受附加的风险。NIST SP800-52提供了关于使用传输层安全（TLS）来保护传输机密性的指导。NIST SP800-77提供了关于使用IPsec来保护传输机密性的指导。NSTISSI No.7003包含了使用保护性分布式系统的指导。相关安全控制：AC-17。

增强控制:

（1）组织使用加密机制来识别传输过程中对信息的泄漏，除非受到另外的可选择的物理措施的保护。

附加增强指导：可选择的物理保护措施包括，例如，保护性的分布式系统。

ICS附加增强指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。相关的安全措施；PE-4,SC-13。

LOW Not Selected	**MOD SC-9**	**HIGH SC-9 (1)**

SC-10 断开网络连接

控制： 在会话结束或［指定：定义的时间段］后，信息系统应终止网络连接。

附加指导： 组织将该控制应用于风险管理中，其中描述了详细的任务或操作要求。

ICS附加指导：一些ICS或组件不允许网络会话中断。在某些情况下，组织认为实施网络会话中断是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：无。

LOW Not Selected	**MOD SC-10**	**HIGH SC-10**

SC-11 可信路径

控制： 信息系统在用户和下列系统安全功能[指定：组织自定义的安全功能，包括最小的信息系统认证和再认证]之间建立一条可信的通信路径。

附加指导：在信息系统和用户的安全功能之间建立的高信任连接使用了一条可信任的路径（例如，登录）。

增强控制：无。

LOW Not Selected	**MOD Not Selected**	**HIGH Not Selected**

SC-12 密钥生成与管理

控制：当在信息系统中需要使用加密系统时，组织采用带有支持程序或人工程序的自动化机制来生成并管理密钥。

附加指导：NIST SP 800-56提供对密钥生成的指导。NIST SP 800-57提供对密钥管理的指导。

增强控制：无。

LOW Not Selected	MOD SC-12	HIGH SC-12

SC-13 密码系统的使用

控制：对于那些需要加密保护的信息，信息系统将执行加密机制，这些机制与可适用的联邦法律、可执行命令、指令、策略、规章、标准、指导相一致。

附加指导：非国家的安全信息系统中，使用加密系统可适用的联邦标准为FIPS140-12（修正版）。由NIST加密模块确认程序（包括FIPS140-1，FIPS140-2，和后来的修正版）来发放的确认证书仍然有效，并且这些模块仍然可继续使用和购买，直到该确认证书被明确废除了。NIST SP800-56和800-57提供了关于密钥生成和密钥管理的指导。有关使用确认证书的附加消息可以在*http://csrc.nist.gov/cryptval*上获得。

ICS附加指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。

增强控制：无。

LOW SC-13	MOD SC-13	HIGH SC-13

SC-14 公开访问保护

控制：组织保护公开信息和应用的完整性和可用性。

附加指导：无。

ICS附加指导：总的来说，ICS不允许公开访问。

增强控制：无。

LOW SC-14	MOD SC-14	HIGH SC-14

SC-15 协同计算

控制：信息系统应禁止协同计算机制的远程激活，并为本地用户的使用提出明确指示。

附加指导：协同计算机制包括，例如，视频和音频会议功能。明确的使用指示包括，例如，当摄像头或麦克风被激活时，给本地用户发送信号。

ICS附加指导：总的来说，ICS中不允许使用协同计算。

增强控制：

(1) 信息系统通过某种支持易用性的方式来提供摄像头和麦克风的物理分离。

LOW Not Selected	MOD SC-15	HIGH SC-15

SC-16 安全参数的传输

控制：信息系统应能在信息系统间提供可靠的安全参数交换。

附加指导：安全参数包括，例如，安全标签和标记。安全参数可能被明确或含蓄地与信息系统中包含的信息联合在一起。

增强控制：无。

LOW Not Selected	MOD Not Selected	HIGH Not Selected

SC-17 PKI证书

控制：组织按照适当的证书策略发放公开密钥证书，或按照从已批准的服务商那获得的适当证书策略来获得公开密钥证书。

附加指导：对于用户认证，每个代理要么建立一个代理认证机构，由联邦的桥认证机构（FBCA）中级或更高级的保证来反复认证，要么使用由已批准的共享的服务提供商提供的认证,像OMB Memorandum 05-24中要求的那样。NIST SP800-32提供了关于公开密钥技术的指导。NIST SP800-63提供了关于远程电子认证的指导。

ICS附加指导：ICS总是分别支持可用性，完整性和加密性。因此，密码学的使用应该是在深思熟虑之后。任何由于使用密码学而产生的潜在因素都绝不应该对ICS的正常操作产生影响。ICS中使用PKI技术应该只支持内部非公开使用。

增强控制：无。

LOW Not Selected	MOD SC-17	HIGH SC-17

SC-18 可移动代码

控制：组织：(i) 为移动代码技术建立使用限制和执行指导，因为可移动代码被恶意使用将对信息系统造成危害；(ii) 授权，监视，并控制信息系统中可移动代码的使用.

附加指导：可移动代码技术包括,例如, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, 和VBScript。使用限制和执行指导既可应用在安装在组织服务器端的可移动代码的选择和使用上，也可以用在个人工作站端移动代码的下载和执行上。控制流程阻止信息系统中无法接受的可移动代码的开发，获取或引入。NIST SP800-28提供了关于活动内容和移动代码的指导.

增强控制：无。

LOW Not Selected	MOD SC-18	HIGH SC-18

SC-19 VOIP

控制：组织:(i) 为VoIP技术建立使用限制和执行指导，因为如果VoIP被恶意使用将对信息系统产生的潜在危害；(ii) 授权，监视，并控制信息系统中VoIP的使用。

附加指导：NIST SP800-58提供关于信息系统中使用的VoIP技术安全因素方面的指导。

ICS附加指导：总的来说，不允许在ICS中使用VoIP。

增强控制：无。

LOW Not Selected	MOD SC-19	HIGH SC-19

SC-20 安全名字/地址解析服务（可信的资源）

控制：提供名字/地址解析服务的信息系统不仅提供为回复解析请求而返回的可信数据，而且附加数据来源和完整性等相关信息。

附加指导：该控制允许远程客户获取源认证和从服务中获得的名字/地址解析信息的完整性保护。域名系统（DNS）服务就是提供名字/ 地址解析服务的信息系统的一个例子；而DNS资源记录就是可信数据的例子。NIST SP800-81提供了关于安全域名系统部署的指导。

ICS附加指导：总的来说，不允许在ICS中使用DNS。使用安全的域名/地址解析服务也绝不能影响ICS的正常操作。

增强控制：当作为分布式的，分等级的域名空间的一部分时，信息系统提供指示子空间（如果子空间支持安全转换服务）安全状况的方法并实现父域和子域之间信任链的检验。

附加增强指导：一种用来指示子空间安全状态的实例方式是使用代理千名人(DS)资源记录(RRs)。

LOW Not Selected	MOD SC-20	HIGH SC-20

SC-21 安全名字/地址解析服务（递归或缓冲分解器）

控制：当有客户系统提出请求时，为本地客户端提供名字/地址解析服务的信息系统，对从可信资源中接受到的解析回复，执行数据来源认证和数据完整性校验。

附加指导：递归或缓冲的域名系统服务器（DNS）就是一种为本地客户端提供名字/地址解析服务信息系统，权威可信的DNS服务器也是可信的资源。NIST SP800-81提供了安全域名系统部署方面的指导。

ICS附加指导：总的来说，不允许在ICS中使用DNS。使用安全的域名/地址解析服务也绝不能影响ICS的正常操作。

增强控制：信息系统为所有的解析回复执行数据起源认证和数据完整性校验，不论本地客户端是否明确请求此服务。

附加增强控制：本地客户端包括，例如，DNS 存根解析。

LOW Not Selected	MOD Not Selected	HIGH SC-21

SC-22 安全名字/地址解析服务的结构和规定

控制：为组织提供名字/地址解析服务的信息系统具有容错能力并执行责任分离策略。

附加指导：域名系统（DNS）就是一种提供名字/ 地址解析服务的信息系统。为了消除单点失效并增强冗余，至少要有两个权威可信的域名系统（DNS）服务器，一个配置成主服务器，另一个配置成次服务器。另外，这两个服务器通常位于两个不同的子网并在地理上是分离的（如，并不位于同一物理设备上）。如果组织的信息技术资源被分成内网资源和外网资源，就要建立具有双重角色（内网和外网）的权威DNS服务器。负责内网的DNS服务器提供关于内部和外部的信息技术资源的名字/地址解析信息，而负责外网的DNS服务器则只提供关于外部信息技术资源的名字/地址解析信息。能访问特定角色的权威DNS服务器的客户端列表也被明确规定了。NIST SP800-81提供了关于安全DNS部署的指导。

ICS附加指导：总的来说，不允许在ICS中使用DNS。使用安全的域名/地址解析服务也绝不能影响ICS的正常操作。

增强控制：无。

LOW Not Selected	MOD SC-22	HIGH SC-22

SC-23 会话认证

控制：信息系统提供通信会话认证保护机制。

附加指导：该控制主要针对会话层通信保护，而不是下层。该控制的意图在于当需要时提供会话层的保护（如，在面向服务的结构中提供基于web的服务）。NIST SP800-52提供了关于使用传输层安全（TLS）机制的指导。NIST SP800-77提供了关于部署IPsec，虚拟专用网（VPNs）的指导以及其他保护通讯会话的方法。NIST SP800-95提供了关于安全web服务的指导。

增强控制：无。

LOW Not Selected	MOD SC-23	HIGH SC-23

类： 系统与信息完整性(SI)
CLASS：OPERATIONAL

SI-1 系统与信息完整性策略与流程

控制：组织开发、发布，并定期检查、更新：1）一个正式的归档的系统与信息完整性策略，策略中标明了目标、范围、角色、职责、管理承诺、组织实体之间的协调关系以及顺从关系；2）一个正式的存档的流程，用来帮助执行系统与信息完整性策略和系统与通信保护相关的控制。

附加指导：系统与信息完整性策略和流程符合适用的联邦法律、可执行命令、指令、策略、规章、标准、指导。系统与信息完整性策略可以包含到组织的通用信息安全策略中，并作为其一部分。可以为一般的安全程序制定系统与信息完整性流程，也可在必要时为特殊信息系统制定系统与信息完整性流程。NIST SP800-12提供了关于安全策略和流程的指导。

增强控制：无。

LOW SI-1	MOD SI-1	HIGH SI-1

SI-2 缺陷修补

控制： 组织识别、汇报并纠正信息系统的缺陷。

附加指导：组织能识别那些包含最近公告的软件缺陷对组织信息系统的影响（和由这些缺陷导致的潜在的脆弱性）的信息系统。组织（或软件开发商/卖主，如果软件是由卖主/订约人开发和维护的）迅速安装最新发布的安全相关补丁，服务包和热调整，安装之前要测试补丁，服务包以及热调整的有效性和对组织信息系统的潜在影响。迅速地标明在安全评估，持续监视，事件回顾过程或信息系统错误处理过程中发现的缺陷。缺陷修复被合并到配置管理中作为紧急更改。NIST SP800-40提供了关于安装安全补丁和管理补丁方面的指导。相关安全控制：CA-2, CA-4, CA-7, CM-3, IR-4, SI-11。

ICS附加指导：NIST SP 800-82中提供了关于ICS漏洞修复方面的指南。

NIST SP 800-82 ICS特别推荐与指南：在ICS环境中对操作系统组件安装补丁需要格外小心。补丁可以修补系统本身的脆弱性，但同时也可能会引入更大的风险。在安装补丁之前一定要经过仔细的测试，并明确可能导致的副作用。补丁更新机制往往是自动的，而对于ICS，应将补丁安装计划在停机的时候进行。

增强控制：

(1) 组织统一地管理缺陷修补程序和自动化升级程序。

(2) 使用自动化的机制定期地，并根据需要来决定关于缺陷修补的信息系统组件的状态。

ICS增强附加指导：这条指南可以应用于措施加强（1）（2）。在某些情况下，组织认为实施自动漏洞修复是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

LOW SI-2	MOD SI-2(2)	HIGH SI-2 (1)(2)

SI-3 恶意代码防护

控制：信息系统执行恶意代码防护。

附加指导：在重要的信息系统条目和出口结点（如，防火墙，电子邮件服务器，web服务器，代理服务器，远程访问服务器）和工作站，服务器，或网络上的移动计算设备上，组织使用恶意代码防护机制。组织使用该机制来检测和清除恶意代码（如，病毒，蠕虫，木马，间谍软件），这些恶意代码是由以下方式传输的：（i）通过电子邮件，电子邮件附件，网络访问，可移动介质（如，USB设备，软盘，光盘）或其他一般方式；（ii）通过利用信息系统的脆弱性。按照组织配置管理策略和流程，当发布最新版本时，组织升级恶意代码防护机制（包括最近的病毒定义）。针对复杂的供应商产品结构（如，使用一个供应商的边界设备和服务器，使用另一个供应商的工作站），组织考虑使用恶意代码保护软件产品。在恶意代码检测和清除过程中，导致了对信息系统的可用性产生潜在的影响，组织也将考虑接受这些误诊误测。NIST SP800-83提供了关于执行恶意代码防护方面的指导。

ICS附加指导：在某些情况下，组织认为实施措施和措施加强是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。NIST SP800-82中提供了ICS恶意代码防护方面的指南。相关安全措施：CM-7。

增强控制：

(1) 组织集中管理恶意代码防护机制。

(2) 组织自动升级恶意代码防护机制。

LOW SI-3	MOD SI-3 (1)(2)	HIGH SI-3 (1) (2)

SI-4 入侵检测工具和方法

控制： 组织使用工具和方法来监控信息系统中发生的事件、检测攻击，并对未授权的系统使用进行鉴别。

附加指导：信息系统的监控能力可通过多种工具和方法获得，（例如：入侵检测系统，入侵防护系统，恶意代码防护软件、日志监控软件、网络监视软件）。在信息系统中（如，在选择的边缘位置，在支持重要应用的服务器群）战略性地部署监视设备来收集基本信息。在信息系统的特定位置也部署了监视设备以追踪特定交易。

另外，这些设备也被用于跟踪安全变更对信息系统的影响。信息收集的间隔时间是由组织基于监视对象以及信息系统支持该活动的能力所决定的。关于所有信息系统的监视行为，组织会咨询适当的法律顾问。当指示对组织的运转，组织的资产，或个体有增加的风险时，组织将根据执法信息，智能信息或其他可信任的信息源，提高信息系统监视活动的级别。NIST SP800-83提供了关于通过多种安全技术检测攻击的指导。NIST SP800-83提供了关于通过恶意代码防护软件检测基于恶意软件的攻击方面的指导。NIST SP800-92提供了关于监视和分析计算机安全日志的指导。NIST SP800-94提供了关于入侵检测和防护方面的指导。相关安全控制：AC-8。

ICS附加指导：监视工具与技术的使用绝不可以影响ICS的正常操作。在某些情况下，组织认为实施措施或措施加强是不合适的（或者产生负面影响，影响安全性，可靠性），组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

增强控制：

(1) 采用通用协议，组织连接并配置单个的网络入侵检测工具，构成涉及整个信息系统的入侵检测系统。

(2) 采用自动化工具来支持实时事件的分析。

(3) 组织采用自动化的工具将入侵检测工具与访问控制机制和信息流控制机制集成起来，通过启用这些机制的隔离和消除攻击的新配置，以对攻击作出快速响应。

(4) 针对未授权和不正常的行为和情况，信息系统监视边界内外的通讯。

附加增强控制：不经常的/非授权的活动或条件包括，例如，恶意代码的出现，信息的非授权输出，或向外部信息系统发送信号。

(5) 当发生下列危胁或潜在的威胁【指定：组织自定义的泄露指示列表】时，信息系统提供实时报警。

LOW Not Selected	MOD SI-4(4)	HIGH SI-4 (2)(4)(5)

SI-5 安全警报和通报

控制： 组织在规定的时间基础上接收信息系统安全警报/通报，给适当人员发布警报/通报，并采取适当的响应行动。

附加指导： 通过文档定义响应安全警报/通报时所应采取的行动类型。组织也维护了与特殊利益群体（如，信息安全讨论会）的约定：（i）促进安全相关信息（如，威胁，脆弱性和最新安全技术）的共享；（ii）提供对来自安全专家的意见的访问；（iii）改进有关安全最佳实践的知识。NIST SP800-40提供了有关监视和发布安全警报和通报的指导。

增强控制：

(1) 组织采用自动化机制，确保在需要的时候，安全警报与通报信息可以有效传递到组织的各个角落。

LOW SI-5	MOD SI-5	HIGH SI-5 (1)

SI-6 安全功能校验

控制: 信息系统校验安全功能的正确操作[选择(一或多个): 系统启动或重启时、具有权限的用户命令时，每隔[指定: 组织定义的时间段]时间]，或者发现异常时，[选择(一或多个): 通报系统管理员、关闭系统、重新启动系统]。

附加指导: 检验安全功能的需求已经被应用到所有安全功能中。对这些安全功能来说，不能执行自动的自我测试，组织既不能执行补偿安全控制，也不能明确的接受那些不能按要求管理的风险。

ICS附加指导: 一般来说，当发现异常时，不推荐关闭重启ICS。

增强控制:

(1) 采用自动化机制来通报失败的自动化安全测试。

(2) 采用自动化机制来管理分布式安全测试。

ICS增强附加指导: 在某些情况下，组织认为实施措施加强是不合适的(或者产生负面影响，影响安全性，可靠性)，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施: PL-2。

LOW Not Selected	MOD Not Selected	HIGH SI-6

SI-7 软件与信息完整性

控制: 信息系统检测与保护软件和信息，以防止对软件和信息的未授权的更改。

附加指导: 对信息系统采用完整性校验应用软件，以查找信息篡改、错误和删除的迹象。采用软件工程实践中商业化的现成的通用完整性机制(例如: 奇偶校验、循环冗余校验、散列加密)，并采用工具自动监控信息系统和应用主机的完整性信息。

ICS附加指导: 在某些情况下，组织认为实施措施或措施加强是不合适的，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。完整性验证程序不应影响ICS的正常运行。相关的安全措施: PL-2。

增强控制:

(1) 组织重新评估软件和信息的完整性，通过【指定: 组织自定义的时间周期】对系统执行完整性扫描。

（2） 组织使用自动工具，通知适当人员在完整性校验过程中发现的不一致。

（3） 组织使用集中管理的完整性校验工具。

LOW Not Selected	MOD Not Selected	HIGH SI-7 (1)(2)

SI-8 垃圾邮件防护

控制：信息系统执行垃圾邮件防护措施。

附加指导：在重要的信息系统条目结点（如，防火墙，电子邮件服务器，远程访问服务器）和工作站，服务器，或网络上的移动计算设备上，组织使用垃圾邮件防护机制。组织使用垃圾邮件防护机制，对由电子邮件，电子邮件附件，internet访问或其他一般方式传输的未经请求的信息进行检测并采取适当行动。针对复杂的供应商设备情况(如，使用一个供应商的边界设备和服务器，使用另一个供应商的工作站)，组织考虑使用垃圾邮件防护软件产品。NIST SP800-45提供了关于电子邮件安全的指导。

ICS附加指导：组织应关闭不用的和不必要的功能和服务(如电子邮件，因特网访问)。由于ICS和通常IT系统运行类型不同，ICS通常并不使用垃圾邮件保护机制。紧急情况下的异常流量可能会被误判为垃圾邮件，给系统造成麻烦或者导致系统失败。相关的安全措施：CM-7。

增强控制：

(1) 组织集中管理垃圾邮件防护机制。

(2) 信息系统自动更新邮件防护机制。

ICS增强附加指导：这条指南可以应用于措施加强（1）（2）。在某些情况下，组织认为实施垃圾邮件保护措施是不合适的(或者产生负面影响，影响安全性，可靠性)，组织应记录下不采用措施的原因，在系统安全计划中记录合适的补偿安全措施，并加以实施。相关的安全措施：PL-2。

LOW Not Selected	MOD SI-9	HIGH SI-9

SI-9 信息输入限制

控制： 组织对授权人员限制向信息系统输入信息的能力。

附加指导：对已授权的个人向信息系统输入信息的限制，可能延伸到由系统使用的特殊访问控制，并包含基于特殊操作/工程责任的限制。

ICS附加指导：相关的安全措施：CM-7。

(1) 增强控制：无。

LOW Not Selected	MOD SI-9	HIGH SI-9

SI-10 信息的准确性、完备性、有效性和可信性

控制： 信息系统检验信息的准确性、完备性、有效性和可信性。

附加指导：对信息的准确性、完备性、有效性和可信性的检验要尽量接近数据源点。用来检验信息系统输入（如，字符集，长度，数字范围，可接受值）的有效语法规则，可以适当地检验输入是否与特殊定义的格式和内容相匹配。到达解析程序的输入将被复查以阻止无意中被当作命令解释的内容。组织政策和操作要求指导信息系统检验信息的准确性、完备性、有效性和可信性的程度。

增强控制：无。

LOW Not Selected	MOD SI-10	HIGH SI-10

SI-11 错误处理

控制：信息系统快速地识别并处理错误，但并不提供可以被敌人利用的信息。

附加指导：组织谨慎考虑了错误信息的结构和内容。错误信息只向授权用户显示。信息系统生成的错误信息提供实时有用的信息，而不显示可能被敌人利用的潜在的危害信息。敏感信息（如，帐号，社会保险号，信用卡号）并不列入日志或相关的管理信息中。组织政策和操作要求指导信息系统鉴别和处理错误情况的程度。

增强控制：无。

LOW Not Selected	MOD SI-11	HIGH SI-11

SI-12 输出信息处理与存储

控制：按照可适用的法律，可执行命令，指令，政策，规则，标准和操作要求，组织处理并保存从信息系统输出的数据，

附加指导：无。

增强控制：无。

LOW Not Selected	MOD SI-12	HIGH SI-12