CISA《2023-2025 年战略计划》（译）

一、概述

（一）目的

本战略计划展现了网络安全和基础设施安全局（CISA）的使命和愿景，促进整个机构与合作伙伴的共同努力，解释了 CISA 作为一个机构的成功之处。它描述了利益相关者、政策和运营环境，并介绍了 CISA 将在未来三年内为更好地执行重要使命而进行的战略变革。战略计划建立在《美国国土安全部 2020-2024 财年安全战略计划》的基础上，并与其保持一致。CISA 将通过该机构的部门和办公室级别的年度运营计划（AOP）实施战略计划。

（二）关于 CISA

CISA 是根据 2018 年《网络安全和基础设施安全局法案》成立的，既是美国的网络防御机构，也是关键基础设施安全和恢复的国家协调员。这一巨大的任务空间需要与世界各地的利益相关方进行接触和建立伙伴关系，并建立强大的国内和区域存在。我们面临的威胁——包括数字的和物理的、人为的、技术的、自然的——比我们历史上任何时候都更加复杂，威胁因素也更加多样化。在我们领导国家努力了解、管理和降低关键基础设施风险的过程中，CISA 是动员集体防

御的核心。我们将竭尽全力，致力于保护美国人民的隐私、公民权利和公民自由。

（三）当前风险形势

国家基础设施和网络面临的风险不断变化，我们的机构必须在这样的复杂环境中执行这一战略计划。日益发展的全球互联网络空间带来了深刻的挑战，我们面临着 24×7×365 的、不对称的网络威胁，而这些威胁对现实世界将带来大规模的影响。

无论使命、行业或部门如何，所有组织都有相同的总体关注点。其中包括对手不断增强的成熟度、能力和胆量；通过高度互联和相互依赖的技术创建的不断扩大的网络攻击面；以及为今天和未来迅速增加高技能网络人才的需要。超越我们的敌人和对手的网络能力是国家安全的当务之急。

网络威胁行为者使用日益复杂的能力来破坏美国经济和民主，窃取知识产权，并挑拨离间。他们利用了政府组织之间的业务界限、公共和私人网络基础设施的复杂性，以及外国对手的资助。CISA 网络防御任务的紧迫性在俄罗斯 2022 年初入侵乌克兰后达到一个极点。

我们促进了与公共和私营部门合作伙伴的有效合作，以确保在面对针对国家基础设施的潜在恶意网络活动时保持警惕，并与这些合作伙伴迅速分享有价值的信息，以帮助建立我们的集体准备。但我们的工作远未完成。缓解网络威胁

需要一种涵盖所有利益相关方的、持续的、全国性的方法。

我们国家物理基础设施的多样性、复杂性和扩展性也带来了独特的挑战。确保关键基础设施、公共集会、选举投票站和关键设施免受恐怖袭击和有针对性的暴力威胁，仍然是一个关键优先事项。气候变化带来的风险同样令人生畏。随着气候事件变得更加极端，我们可以预期自然灾害、稀缺性和系统压力将给我们国家的基础设施带来进一步的压力，这将需要更加关注从灾难中复原的能力。这些风险也增加了当地应急人员和政府官员在事故和事件期间的压力。在下一次灾难发生之前，他们必须拥有弹性的、可互操作的通信系统。

当然，威胁和风险并不局限于单个系统或实体。支撑我们国家关键职能（National Critical Functions，NCF）的基础设施跨越多个部门，并会变得更加相互依存。NCF 属于美国至关重要的政府部门和私人部门的职能，其破坏、出错或功能失调将对安全、国家经济安全、国家公共卫生或安全或其任何组合产生破坏性影响。因此，国家的网络和物理基础设施之间的界限越来越模糊。信息物理技术和系统的融合为从制造业到医疗保健到交通运输等提供了关键功能，这意味着单一事件可能表现为多个行业的服务损失或降级。操作技术（OT）和工业控制系统（ICS）带来了独特的风险，需要特别关注，因为与某些安全控制相关的大规模部署一旦受到干扰或挑战，后果更为严重。虽然新技术和新兴技术是创新和

机遇的重要驱动因素，但它们也可能带来无法预料的风险。同样，不可预见的相互依赖性可能导致系统性风险状况和层叠效应。这种不断变化的环境需要比以往任何时候都更加统一的方法。

在这个动态的风险环境中，我们必须有智慧、创新性和适应性。应对这些挑战需要一支强大的员工队伍，作为一个统一的机构进行协作。我们致力于成为联邦政府的首选工作场所，拥有高绩效的员工队伍。随着我们更加整合和灵活，我们还将不断努力改善我们的业务运营。我们一起作为一个团队和“一个 CISA”而存在。

（四）任务和愿景

我们的任务是“领导美国理解、管理和降低其网络和物理基础设施的风险”，我们的愿景是“为美国人民提供安全和弹性的基础设施”。

（五）CISA 核心价值观

CISA 的定位与众不同，其并不是成立另外一个官僚机构，而是一个更类似于开展公私合作的机构。核心价值观包括:

（1）协作

强有力和充满活力的伙伴关系对 CISA 所做的工作至关重要。CISA 将把每一次合作都视为与队友、合作伙伴和客

户建立信任的机会。

（2）创新

CISA 必须以创造力和敏捷性前进，走在对国家和生活方式的威胁前面，必须以弹性为基础。

（3）服务

CISA 被定义为无私地为美国人民服务；其承诺不仅仅是一项使命，更是一种号召，要保护和捍卫美国人民每时每刻所依赖的基础设施。

（4）责任

每个人都应积极主动地承担起自己的使命，并为自己的行为负责，还将通过信任、透明和彻底的诚实来增强员工的能力。

（六）CISA 核心原则

CISA 将秉持以下核心原则：

（1）以人为本；

（2）永远做正确的事；

（3）以同理心领导；

（4）寻求并提供诚实反馈；

（5）透明有效的沟通；

（6）建立并培养关系网络；

（7）想象、预期、创新求赢；

（8）发挥效用；

（9）培育归属感、多样性、包容性和平等;

（10）博弈;

（11）保持战斗;

（12）终身学习。

二、战略计划

该战略计划确定了四个目标，这些目标将推动 CISA 实现我们作为一个统一机构的使命。与每个目标相关联的是详细说明我们将如何实现这些目标并评估我们的成功。图 1 描述了我们的战略框架。在接下来的章节中，预期成果和评估方法突出了每个目标的成功之处。CISA 正在制定绩效和有效性的具体措施，这些措施将在我们的年度运营计划（AOP）中定义。确定适当的措施并不是一项简单的任务。这将需要在整个计划执行期内持续努力，我们将根据需要对其进行完善。

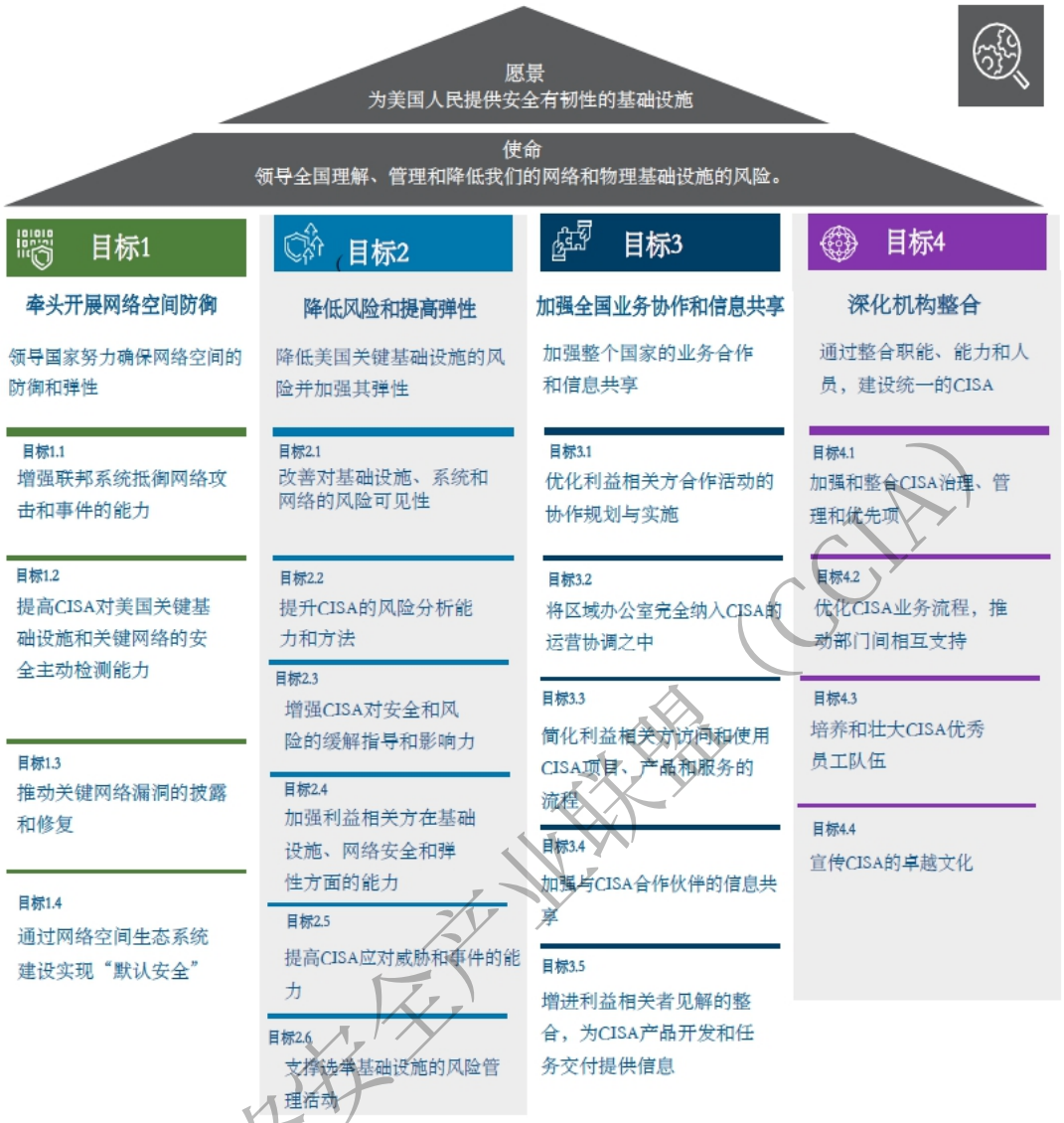

图 1 战略计划概要图

（一）目标 1：牵头开展网络空间防御

CISA 作为美国的网络防御机构，领导全国防御针对美国关键基础设施、联邦和各级政府、私营部门和美国人民的网络威胁。CISA 必须在网络防御任务中更加协作、主动降低风险。与许多合作伙伴共事，CISA 的责任是帮助减轻国家 NCF 最重大的网络风险，无论是在这些风险出现时还是在重大事件发生之前。

CISA 专注于最大限度地减少试图渗透、利用、破坏或摧毁关键基础设施系统和网络以及它们所支持的 NCF 的影响。我们将作为联邦民事行政部门（FCEB）网络安全的业务领导和联邦网络安全共享服务提供商推进我们的工作。我们必须确保联邦民事机构能够获得最好的网络安全工具、事件响应支持和风险管理能力，以保护维持我们国家基本运作的网络。

既然我们无法减轻看不到的风险，我们将积极搜寻网络威胁，并与网络安全社区合作，推动关键漏洞的披露和缓解。此外，我们必须在更广泛的网络生态系统中推进安全。未来，推动软件和硬件在设计和构建时将安全性作为首要任务是必要的，特别是在直接支持关键功能的 ICS 和 OT 中。除了安全技术，还必须解决我们网络生态系统中的劳动力短缺问题，包括确保我们的网络安全劳动力反映我们国家的多样性，并准备好迎接未来挑战。

作为国家的网络防御机构，有效的公共和私营部门伙伴关系和协作是至关重要的任务，也是实现安全和有弹性的网络生态系统的唯一途径，为创新和繁荣的国家提供动力。

目标 1.1：增强联邦系统抵御网络攻击和事件的能力

CISA 致力于帮助联邦机构进行必要的大胆变革，以改善国家的网络防御态势。通过推动和促进采用现代、安全和弹性技术，提高事件响应能力，约束联邦政府的供应链风险，

以及提高对联邦网络中网络威胁的可见性。CISA 将最大限度地利用权力，推动和衡量联邦民事机构采用强有力的网络安全行动。CISA 还将通过提供可扩展和创新的服务和能力，帮助各机构建立有效的安全计划。

预期成果:

（1）联邦民事行政部门已准备好并能够从网络攻击和事件中快速恢复。

（2）联邦民事行政部门在网络攻击和网络安全事件发生期间和发生之后保持业务的连续性。

评估方法:

CISA 将评估联邦机构对 CISA 网络防御指南、标准和指令的遵守情况和实施效果，以改善国家的网络防御态势。

目标 1.2：提高 CISA 对美国关键基础设施和关键网络的安全主动检测能力

美国正面临着来自高水平敌人的威胁，该类敌人寻求对有价值的系统和信息的持续访问。CISA 检测和预防威胁的能力取决于显著扩大行动可见度。CISA 将提高其在联邦和各级政府网络中主动检测威胁的能力，同时与行业伙伴合作，以增强针对专用网络的威胁的理解。CISA 将不断提升威胁搜寻能力，以快速协调大规模威胁识别和缓解。

预期成果:

（1）CISA 为美国的网络防御者提供更多的具有指导性检测信息。

（2）美国的网络防御者能够在破坏性入侵发生之前，主动缓解其关键网络上的威胁。

评估方法:

CISA 将衡量网络监测、网络威胁分析和网络威胁狩猎等方面工作的有效性，以减少检测时间和恢复时间。

目标 1.3：推动关键网络安全漏洞的披露和缓解

CISA 意识到每个硬件和软件都存在漏洞，并作为可信任的合作方协调新漏洞的披露，以减少对手可利用的漏洞。CISA 将与各类网络安全研究团体密切合作，鼓励识别和报告未知漏洞，并大力推动缓解措施。CISA 与合作伙伴一起，通过相关渠道和机制，实现及时和协调的漏洞披露、提供建议，并扩大适当的缓解措施。为了降低未知漏洞的频率和规模，CISA 还必须利用权力和能力来识别未缓解的漏洞，特别是影响关键基础设施的漏洞，并在漏洞被利用之前推动紧急缓解措施。最后，CISA 将与网络安全界合作，利用网络安全审查委员会（Cyber Safety Review Board）和其他咨询机构的经验教训和建议，提升美国的网络安全水平。

预期成果:

（1）关键基础设施所有者/运营商增强网络安全漏洞的透明度。

（2）关键基础设施所有者/运营商能够在漏洞被利用前协调和整合缓解措施。

评估方法:

CISA将评估CISA的网络漏洞评估和修复服务的利用率和有效性，以增加漏洞的识别和缓解，减少敌手利用关键基础设施的窗口。

目标1.4: 推进网络空间生态系统建设，以实现“默认安全”

全美各地的公共和私人网络防御者依靠许多常用工具、流程和资源来开展工作。CISA 鼓励开发和采用最新技术的网络防御和网络运营工具、服务和能力，以推动技术生态系统中的“默认安全”。CISA 还将为技术提供商和网络防御者提供支持，帮助他们确保软件和硬件产品、服务、网络和系统的安全性。CISA 意识到安全的网络生态系统既关乎技术，也关乎人，CISA 将通过自身的网络教育资源，赋能全国网络劳动力，以填补关键技能的短缺。最后，CISA 意识到技术产品的设计和开发必须优先考虑安全性，默认采取强有力控制手段，并减少可利用漏洞的扩散。

预期成果:

（1）广泛用于国家关键职能（NCF）的技术产品在设计上具有安全性和弹性。

（2）国家的网络和系统在默认状态下更加安全。

评估方法：

CISA 将评估技术产品和服务中安全开发实践和控制的采用和有效性。

（二）目标 2：降低风险和提高弹性

CISA 协调全美保护和防范关键基础设施风险。这项全国性工作的核心是确定哪些系统和资产对国家真正至关重要，了解其脆弱性，并采取行动管理和降低其风险。CISA 是关键基础设施所有者和运营者的重要合作伙伴，帮助其降低风险和建立安全能力，以抵御来自网络攻击、自然灾害和物理上的威胁和破坏。关键基础设施分为 16 个行业[1]，每个行业都有一个指定的行业风险管理机构（Sector Risk Management Agency，SRMA），负责帮助拥有者和运营者管理该行业的风险。CISA 担任 16 个指定关键基础设施行业中 8 个行业的 SRMA[2]，为这些行业的风险管理工作发挥独特的伙伴作用。

CISA 还通过协助识别和管理风险、提供 CISA 拥有的能力和资源，支持其他 SRMA 的安全和弹性。无论是作为多个行业的 SRMA，还是作为其他 SRMA 的支持者和促进者，CISA 在保护我们国家最关键的基础设施方面都发挥着关键

[1] 《总统政策指令-关键基础设施的安全性和弹性》确定了美国 16 类关键基础设施行业，包括：化学、商业设施、通讯、关键制造部门、水库大坝、国防工业基础部门、紧急救援部门、能源部门、金融部门、食品和农业部门、政府设施、医疗保健和公共健康部门、信息技术部门、核反应装置材料和废弃物、交通运输系统、水供应和污水处理系统。

[2] CISA 担任化学、商业设施、通讯、关键制造部门、水库大坝、紧急救援部门、信息技术部门，以及核反应装置材料和废弃物等 8 个行业的 SRMA。

作用。

为了更好地满足我们利益相关者的不同需求，并将我们的努力集中在国家最关键的基础设施上，CISA 必须进一步加深对国家当前和未来关键基础设施风险的理解。我们使用 NCF 来识别和分析风险，简单地说，就是我们需要关键基础设施该做的事，来实现国家安全、经济安全以及公共卫生和人身安全。我们使用 NCF 来构建分析，告诉我们实体、资产、系统、技术和商品中的风险集中之处，这样我们就可以将精力集中对降低国家风险发挥最大作用的地方。

这种方法使我们能够预测潜在的层级效应来源，并在当今互联基础设施环境中规划有效的缓解措施。当威胁和危险出现时，我们必须已经在操作上做好准备，以协助我们的合作伙伴进行事件管理和恢复，包括在重大网络事件和重大灾难期间。通过加强我们的自愿伙伴关系，并根据适用的监管责任，包括化学设施反恐标准（CFATS），CISA 将推进安全解决方案，解决国家关键基础设施面临的最紧迫的风险。例如，通过化学设施反恐战略方案，高风险化学设施必须采取措施，检测、延迟和应对物理和网络攻击，如设立安全官员；设置障碍和准入控制措施；实施入侵检测能力；制定针对物理攻击和网络攻击的事件报告、响应和调查计划等措施。

目标 2.1：扩大对基础设施、系统和网络的风险可见性

CISA 在收集正确的数据的基础上，努力理解关键基础设施风险，促进 CISA 推动评估、分析和决策。这需要 CISA 深入了解国家的网络和关键基础设施的物理资产及系统，并识别可能影响该基础设施的潜在和未来风险来源。CISA 必须巩固其作为国家关键基础设施数据的国家级权威和中央知识库的角色。CISA 将发展其工具、条令和作战能力，以及评估基础设施危急程度的业务能力，全面识别关键基础设施，并了解基础设施的脆弱性。CISA 将部署创新工具并推进合作伙伴关系，以获得对网络和物理威胁和漏洞的可见性。CISA 将不断识别新兴风险，以免对基础设施构成威胁。最后，随着 2022 年《关键基础设施网络事件报告法案》（Cyber Incident Reporting for Critical Infrastructure Act of 2022, CIRCIA）的通过，CISA 正在改善政府对网络事件的关注，以便 CISA 和其它机构可以与利益相关方合作，采取行动来更好地保护其免受类似事件的影响。

预期成果:

（1）CISA 是关键基础设施的中央数据库和国家权威机构。

（2）CISA 能够在新风险对关键基础设施构成威胁之前，识别出新兴风险。

评估方法:

CISA 将评估在风险可见性和关键基础设施的安全性上

的提升情况。

目标 2.2：提升 CISA 风险分析能力和方法

网络防御和基础设施安全任务成功的基础是了解国家级和行业级风险，特别是针对关键系统、网络和基础设施的系统性风险。CISA 必须具备成熟的风险分析能力和方法，以促进其深入了解所面临的风险。在目标 2.1 扩大可见度的基础上，CISA 将确保将关键基础设施信息和识别工作纳入分析方法，以产出能够指导机构决策的全面、综合的分析结果。利用 CISA 分支拥有的独特技术专长，为特定项目提供定制的风险分析能力，以支撑处理跨部门战略级别的优先风险。

预期成果:

（1）CISA 具备可定制的风险分析能力和方法，以促进深入了解。

（2）CISA 以综合威胁图谱来指导和确定行动的优先级。

评估方法:

CISA 将评估 NCF 风险分析的成熟度，以及风险数据的跨机构可访问性。CISA 还将衡量其对 SRMA 评估行业风险的支持情况。

目标 2.3：增强 CISA 对安全和风险的缓解指导和影响力

为了加强对关键基础设施的保护，使其免受威胁、危害

和风险，CISA 为利益相关方提供安全和风险缓解指导及协助。为了改善和扩大 CISA 降低风险的影响，CISA 将提供可操作的专业知识和缓解措施，以定位基础设施安全威胁和强化应急通信系统，CISA 将发布权威指南以推动有效的 IT 网络风险管理。CISA 将把本指南的重点放在对我们的利益相关方至关重要的风险上，以及 CISA 确定的优先事项。

在适当的情况下，CISA 将制定内部标准和建议，以指导安全决策，正如其建立绩效目标和提高跨部门网络安全基线。CISA 将确保高风险化学设施符合 CFATS 和其他适用法规的安全要求。在适当和有授权的情况下，CISA 还将提供有针对性的技术援助或评估，以有效提高安全性和弹性。

预期成果:

（1）利益相关方采用 CISA 的关键基础设施安全指南、标准、性能基准和风险管理专业知识。

（2）高风险化学品设施符合基于风险的性能标准。

评估方法:

CISA 将评估利益相关方采用 CISA 的物理、应急通信和网络安全指南的情况和效果。

目标 2.4：加强相关利益方在基础设施、网络安全和的弹性方面的能力

CISA 作为一个值得信赖的合作伙伴，帮助关键基础设施所有者和运营者建立能力，就其自身的安全性和弹性做出

风险精确决策。为了更好地满足他们的需求，CISA 必须适当调整在网络安全、基础设施安全和应急通信方面的关键计划和风险相关产品，以满足不断增长的利益相关方的需求。这将包括 CISA 作为 SRMA 的职责，以及为其他部门和机构的 SRMA 职能提供的支持。CISA 将提供有效的能力和服务，以应对利益相关方最紧迫和不断变化的物理安全挑战，其中包括内部威胁、枪击事件、爆炸预防和公共集会场所的安全。CISA 还必须响应紧急需求，调整产品以应对新的风险，例如提供专门针对这些系统所面临的网络安全风险的新应急通信产品。能力建设还需要将 CISA 的产品扩展到新的利益相关方，并将 CISA 内的网络安全服务扩展到非联邦利益相关方。

预期成果:

（1）CISA 的能力建设产品和服务可满足不断增长的需求。

（2）SRMA 和其他利益相关方认为 CISA 的产品和服务具有影响力、及时性和针对性地满足需求。

评估方法:

CISA 将评估不同利益相关方群体可获得的关键产品和服务的增长和影响。

目标 2.5: 提高 CISA 应对威胁和事故的能力

CISA 维护一个 24/7/365 作战态势和响应协调中心，以

协调、综合的方式应对发展中的网络和物理事件或威胁。CISA 必须加强和扩大总部和区域能力，以能够在实际威胁和事件中支持利益相关方和机构合作方，包括恐怖主义、有针对性的暴力袭击和重大自然灾害等。这包括了 CISA 作为八个关键基础设施部门的 SRMA 的角色，以及对其他部门和机构的 SRMA 只能的支持。在重大网络事件期间，CISA 随时准备支持公共和私人实体的响应工作，包括在适当的情况下部署可用的事件响应能力，以限制负面影响，最大限度地减少运营停滞时长，并实现快速恢复。对于国家和地区重大事件，如自然灾害，CISA 同样会酌情部署可用资产和专业知识，包括 CISA 为应急响应人员提供支持的职责，依据在国家应对框架中的应急支持职能 2 和应急支持职能 14。此外，CISA 将扩大重要的紧急通讯支持服务的覆盖范围，以确保第一响应者的呼叫能打通，并且公共安全实体可以在事件期间快速相互通信。

预期成果:

（1）CISA 支持利益相关方具备针对不断发展的威胁和事件做出快速、适当响应的能力。

（2）CISA 确保关键基础设施的连续性和弹性。

评估方法:

CISA 将评估关键应急通信服务的效率和使用情况，以

及 CISA 的事件响应能力。

目标 2.6：支撑选举基础设施的风险管理活动

各级政府都进行选举。作为选举基础设施的 SRMA，CISA 是联邦政府掌握和识别选举基础设施风险的中心，并确保选举官员及其私营部门合作伙伴拥有管理其系统风险所需的信息。凭借与选举官员和供应商的自愿合作伙伴关系，CISA 从针对联邦合作伙伴（如联邦调查局、美国选举援助委员会和情报部门）提供的服务和评估的中收获了独特的见解。

CISA 利用这些见解来推动机构的指导，并为风险管理行动提供信息。随着风险形势的发展，CISA 的支持已从关注网络安全发展到更广泛的风险管理方法，以平衡网络、物理和运营安全。这包括将现有资源和能力有效应用于选举基础设施细分行业的风险管理活动，以及针对该细分行业独特的风险状况开发新产品。CISA 还支持州和地方官员解决其社区中的错误和虚假信息。

预期成果：

（1）CISA 的服务、产品和指导能够响应利益相关方的需求，并根据其对选举基础设施风险的不断理解进行迭代改进。

（2）从风险和脆弱性趋势中吸取的经验教训适用于整个选举基础设施。

评估方法：

CISA 将评估其对各级政府和私营部门选举利益相关方的影响程度，并提供适合其风险状况和组织能力的产品和指导。

（三）目标 3：加强全国业务协作和信息共享

政府和私营部门之间的信任、持续和有效的伙伴关系是我们共同努力保护国家关键基础设施的基础。我们的安全和保障依赖于关键基础设施部门的共同承诺和投资。通过我们与联邦机构和其他机构的合作伙伴关系，CISA 将扩大和加强这些共同承诺，提供产品和服务，使对基础设施安全和弹性的持续投资成为明智和容易的选择，并加强地方、地区和国家层面的信息共享和协作。我们将充分利用我们的召集权和关系管理能力，扩大和完善与利益相关方的伙伴关系，并促进信息共享。

我们将以谦逊、透明、感恩、以及增加价值的坚定决心对待每一个合作。

这需要地方、区域和国家的存在和积极参与。它还需要开发一个可识别的 CISA 品牌，并可靠地履行我们的品牌承诺，以捍卫和保护关键基础设施。我们将履行保障关键基础设施安全和韧性的国家协调员一职，根据《全国基础设施保护计划》（National Infrastructure Protection Plan）中定义的伙伴关系结构，让行业风险管理机构（Sector Risk Management

Agencies，SRMAs）和关键基础设施部门参与进来。利用 CISA 自身的召集权力和关系管理能力，积极扩大和加强共同责任，提供产品和服务，提高地方、区域和全国层面的信息共享和协同程度。

CISA 职能专家和支持人员在提供 CISA 产品、服务和信息的同时，还收集利益相关者的反馈，以不断完善自身、及时了解自身关注的领域。在我们的整个参与过程中，无论是一对一还是多对多，我们都将为公众、我们的合作伙伴和利益相关方提供价值，同时积极保护他们的隐私、公民权利和公民自由。

目标 3.1：优化利益相关方合作活动的协作规划与实施

为了优化 CISA 和利益相关方的参与和合作价值，我们必须在我们的部门、SRMA 和更广泛利益相关者社区内规划、优先考虑和协调利益相关者的参与。我们将在我们所服务的利益相关者中建立我们的 CISA 品牌，目标是培养对我们带来的价值的信心。我们将利用利益相关方的数据和见解、客户需求信号、运营要求和领导层的优先事项来指导国家和地区层面的外延活动的发展；优先考虑有针对性的区域、特定主题和基于部门的参与；以及定制个别客户参与。我们将履行立法和政策授权，的领导，作为 SRMA 和关键基础设施安全和弹性的国家协调员，领导基于行业的合作。我们将与之前定义的所有 CISA 利益相关方合作，其中也包括弱势群体。

预期成果:

（1）作为关键基础设施安全和弹性的国家协调员，CISA 的参与、伙伴关系和协调工作是有针对性、有目的和优先的。

（2）CISA 和利益相关方的关系不断增进。

评估方法:

CISA 将评估战略性的利益相关方参与情况和伙伴关系活动的效能。

目标 3.2：将区域办事处完全纳入 CISA 的运营协调

CISA 的区域办公室职员对于成功开展外展服务至关重要：他们改善了 CISA 产品和服务的获取途径，建立了合作伙伴关系，在全国范围内降低风险、改善复原能力。CISA 将加强总部与区域员工之间的整合，建立协调总部各部门和区域之间的活动流程，并且相互支持运营关系管理。为了优化 CISA 计划、产品和服务的交付，我们将加强现有国家级与地区之间伙伴关系管理框架的联系，直接将行业和政府协调委员会（SCC 和 GCC）等要素扩展到适当地区。CISA 还将创建内部业务管理论坛、机制和流程，使全国范围内的利益相关方参与规划和协调变得简单、高效和互利。

预期成果:

（1）CISA 总部和区域运营部门共享相同的操作画面。

（2）地方和区域利益相关者的问题和关切能够在 CISA 及其协作组织内恰当地提出。

评估方法:

CISA 将评估区域和总部协调活动的整合，以及区域利益相关方参与的影响。

目标 3.3：简化利益相关方访问和使用 CISA 项目、产品和服务的流程

CISA 的项目、产品和服务为利益相关方提供了必要的洞察力，使其能够在资产、系统和企业层面针对网络和物理基础设施风险降低、防御和弹性做出及时而明智的决策。为了能够有效和方便地使用这些资源，CISA 致力于在允许的情况下根据客户的具体需求和情况，为其提供量身定制的产品信息、访问权限和交付。为此，CISA 的资源目录将始终可用、准确、可定制、有吸引力且易于访问。我们将在整个机构内广泛和一致地推广我们的项目、产品和服务，以扩大我们在核心利益相关者群体中的影响力，同时增加未被充分代表的群体和非传统利益相关方的合理获取和使用。

预期成果:

（1）利益相关方可以快速找到并访问 CISA 产品和服务。

（2）CISA 主动告知利益相关方恰当的产品和服务。

评估方法:

CISA 将评估部门项目、产品和服务的质量以及可访问性。

目标 3.4：增强与 CISA 合作伙伴的信息共享

为了提高 CISA 及其利益相关方的态势感知能力，CISA 将加强与外部伙伴的多向沟通，包括及时报告事件，共享威胁、漏洞、情报及其他信息和数据等。促进更大范围的信息共享需要继续建立新的协作结构，如联合网络防御协作体（Joint Cyber Defense Collaborative，JCDC），它与 SRMA 和联邦网络中心合作密切。CISA 尚在完善现有架构，如联邦高级领导委员会（Federal Senior Leadership Council，FSLC）、信息共享和分析组织（Information Sharing and Analysis Organizations，ISAO）、信息共享和分析中心（Information Sharing and Analysis Centers，ISAC）、以及 SCC 和 GCC。这将使利益相关方能够更好地及时应对事件。

增强（Enhancement）意指加快速度、提高准确性，实现信息共享和协作的有效性，同时利用 CISA 的权威来保护隐私、公民权利和公民自由。

预期成果：

（1）利益相关方可以获得及时、相关和准确的决策参考信息。

（2）CISA 的数据处理和信息共享能够保护隐私、公民权利和自由。

评估方法：

CISA 将评估与合作伙伴进行多向信息共享的意义。

目标 3.5：增进利益相关方意见的整合，为 CISA 产品

开发和任务交付提供信息

来自外部利益相关方的见解有助于改善 CISA 的产品和服务，使任务得以交付。一些利益相关方以访谈或事后反馈的形式提供直接反馈。其他则更多地提供间接见解，例如通过合作的伙伴或从评估数据中获取经验教训。

CISA 将积极征求利益相关者的反馈意见，不断完善和改进产品以提供切实的价值。CISA 将加强利益相关方见解、信息和数据的整合，以协助决策及产品、服务和重点领域的优化、开发、修改和定制。

预期成果:

（1）利益相关方能够反馈其需求、兴趣和优先事项。

（2）CISA 适当采纳利益相关方的反馈意见，以改进产品、服务的开发和交付。

评估方法:

CISA 将评估利益相关方的满意度和反馈，以持续改进。

（四）目标 4：深化机构整合

CISA 必须统一为一个机构工作。这意味着我们必须简化现有的运营，并采用灵活的新技术，以改善客户服务。通过提高治理和管理水平、优化组织，我们将打破组织孤岛，增加我们服务的价值，并提高利益相关者的满意度。此外，我们必须为我们的员工提供支持和授权。人才是 CISA 最宝贵的财富。CISA 专注于创造一种组织文化，在这种文化中，

人们热爱所做之事，尊重同事，被其领导授权，并感觉他们每天都在发挥价值。我们将文化视为我们使命成功的关键。

成功更多地取决于释放人的力量和潜力，而不是技术。CISA 正在建立一种卓越的文化，这种文化重视核心价值观和核心原则，包括团队合作和协作、创新和包容、所有权和授权、透明度和信任。即使我们专注于培养今天的劳动力，也要认识到我们的努力在帮助建立未来的劳动力方面也发挥着重要作用，特别是增强网络劳动力以应对网络防御挑战。

目标 4.1：加强和整合 CISA 治理、管理和优先项

CISA 致力于在保全整合的专业知识、明确的责任界限和团队身份前提下，成熟并战略性地解决阻碍我们高效交付的孤岛。我们将通过实施 CISA 各级跨任务授权办公室（MEO）会议和交流计划，并建立治理和管理结构，提供必要的数据和流程，以实现优先决策。CISA 将努力划定工作范围，分配组织和/ 或个人的责任，以推动集体决策，并记录和整合流程，以确保最佳实践的标准化和利用。

我们将更好地把规划、计划、制定预算、执行和评估（PPBEE）流程整合到 CISA 治理流程和决策中，以继续成为公共资金的好管家，为基本运营职能（如工资、发票等）提供有效的内部控制，并支撑明智的投资决策。随着 CISA 的发展，我们将战略性地提供额外的 MEO 资源，以便 CISA 在必要时扩大能力，以更好地实现我们的使命。

预期成果:

（1）CISA 将领导愿景转化为积极行动。

（2）CISA 具有战略性且透明地分配资源，以支持 CISA 集体的高效交付。

评估方法:

CISA 将评估资金的有效性和透明度情况，以及 CISA 整体的项目和流程的标准化和整合程度。

目标 4.2：优化 CISA 业务流程，推动部门间相互支持

CISA 的业务运作能力至关重要。根据需要，我们将简化现有运营，并采用灵活的新技术，改善客户服务。在整个 CISA 中，我们将推进提高被证明有效的产品、服务和资源的利用率，包括安全、创新且可操作的技术解决方案，帮助实现运营成功。我们将整合系统和数据，以提高态势感知能力，提供可付诸行动的信息以支持领导决策，改进流程和协作，具备成熟的信息共享和数据管理能力。

预期成果:

（1）CISA 高层领导和经营者拥有一致、及时的态势感知和可付诸行动的信息。

（2）CISA 完整整合组织内的系统、流程、数据和架构。

评估方法:

CISA 将评估内部系统、流程和架构在增强组织内的多向支持方面的效用。

目标 4.3：培养和壮大 CISA 的优秀员工队伍

国家需要优秀的 CISA，我们义不容辞。CISA 员工必须拥有适当的证书、专业知识和技能并应用。我们将在成功培养和发展劳动力和文化的基础上，吸引和留住我们国家最有才华的网络和基础设施捍卫者。CISA 的人才生态系统将涵盖招聘、雇用、培训、认可、晋升、留任和继任，还将积极发现和培养非传统领域的潜在人才，从各个领域背景中寻找人才。我们将优先考虑并利用国土安全部的网络人才管理系统，使我们的招聘和雇用工作现代化。

为促进员工留任，CISA 还将保证所有级别的员工和领导都有平等的职业发展和教育机会，创造有助于培养高绩效团队的环境。我们将在整个组织内优化我们的指导和辅导，同时奖励优秀员工。我们将通过提高透明度和运营效率，创造一个高绩效团队能够蓬勃发展的环境。创造更稳健的职业发展道路和开发更多跨部门的职业发展机会，为我们的员工创造公平的结果。这也将确保当下和未来的网络防御者训练有素。

CISA 制定了“CISA 网络创新研究员（Cyber Innovation Fellow）倡议”，该倡议为私营部门网络安全专家提供了参与本机构网络安全运营团队的机会，有助于 CISA 的使命和自身的专业发展。研究员将帮助设计 CISA 的网络安全计划和服务实施方案，并为支持联邦网络安全的传统项目设计新方

法（包括人工智能、机器学习和云安全等）。

预期成果:

（1）CISA 招聘、培训和留任熟练、多样化和高绩效的员工。

（2）CISA 认可、促进并为员工提供有意义的职业发展道路。

评估方法:

CISA 将评估员工的雇用、留任情况，以及员工培训发展情况。

目标 4.4: 宣传 CISA 的卓越文化

CISA 文化的力量对实现使命至关重要，也是我们作为一个 CISA 成功的基础。我们将继续通过传播核心价值观和核心原则来建设文化。我们的文化将融入到日常任务、使命、功能、服务、日常行为中。

我们将优先创造一个心理安全的环境，让人们能够做真实的自己；员工感到被关心、被支持、被赋权，感到尊严和尊重；实行问责制。我们将优先考虑健康，以及通过系统地减轻倦怠和提供获得心理健康资源的途径，提高整个机构的弹性。推进公平和公正的组织文化要求 CISA 领导提高奖励、决策结果、沟通和员工待遇方面的透明度和公平性。为了提高组织绩效，CISA 将培养一个鼓励反馈、学习、成长和创新观点的环境。

卓越文化将使CISA成为网络社区公认的领导者，并成为在联邦政府部门工作的首选目的地。

预期成果:

（1）CISA在网络防御和保护关键基础设施方面发挥的作用获得国家认可。

（2）CISA的文化根基——包括健康、心理安全、创新、责任和对使命的热情等，得到认可、实践并强化。

评估方法:

CISA将评估员工的心理安全、多样性和倦怠情况的改善，这对于形成创新和积极的文化至关重要。

（供稿单位：北京升鑫网络科技有限公司）