编者的话

2012 年 12 月 19 日，美国总统奥巴马签署了《信息共享与信息安全国家战略》（后文简称“信息共享战略”），战略认为美国的国家安全取决于向正确的受众提供所需信息的能力。延续 2010 年颁布的《国家安全战略》思路，“信息共享战略”在信息共享的流程、标准和技术方面，提供了更具整合性与更加有效的政策指导。

《信息共享与信息安全国家战略》对信息共享的范围未作规定，没有明确定义具体哪一类或哪一种信息必须被共享；相反，将政策重点转移到如何识别信息需求来支撑政府的有效决策。总结过去几年信息共享取得的经验，虽然提高了美国的创新能力，但日益增多的共享信息也急剧凸显了缺陷漏洞的风险，因而需要进一步加强对信息的保护力度。

面对这些挑战，“信息共享战略”制定了战略性的应对方案，并以三个核心原则为出发点：首先，将信息视为国家资产；其次，信息共享和信息安全需要进行共同的风险管理；再次，支撑政府有效决策的信息需求，构成本战略所有行动的基础，信息共享的首要目的就是为了能够更科学有效地做出决策。基于这三个原则，本战略重点关注实现五方面的目标：（1）加强结构治理，明确各级政府职责与需求，落实责任制来促进多方合作。（2）推动通用标准与数据“标识”的使用，提高数据关联性与用户获取数据的效率，继续完善身份认证和授权控制，提升信息安全保障能力。（3）共享联邦政府 IT 服务，改善数据、网络的互操作性，以及提高政府的采购效率，来优化信息技术对行政职能支撑的有效性。（4）推进信息共享与保护政策的标准化，实施监测自动化等技术解决方案，来加强对信息的保护。（5）保护隐私权、公民权和公民的自由。

《信息共享与信息安全国家战略》虽然对信息共享只是提出了概要性要求，未详述战略的保障执行机构，但结合已取得进展，就共享流程、标准和技术方案进行了更为细化的政策指导，后续出台的战略实施计划值得我们持续关注。

责任编译：贾一苇

目　录

美国信息共享与信息安全国家战略

致辞

作为美国总统，没有比确保国家及人民安全更重大的责任了。为了满足这一职责，就需要我们的各个职能部门，包括情报机关、军队、外交部、国土安全部、执法部门、公共健康部门，以及我们在各州、各地方以及各私人部门中的全体合作伙伴，开展紧密合作和通力配合。相应地，这种合作需要及时、有效的情报和信息共享，需要将对我们国家有威胁的情报和信息及时并有效地传达给所有需要知晓的人——上至总统，下至街头的巡逻警察。

自2001年9月11日以来，我们在信息共享方面已经取得了可观的进步。今天，我们的分析家、调查者以及公共安全专家们正在以前所未有的效率共享着更多的信息，开展着更紧密的合作。但是，由于一些关键信息没有快速共享或者没有广泛传播，以及一些机密、敏感信息因未授权泄漏，对国家安全造成了严重影响。

《信息共享与信息安全国家战略》（以下称为本“战略”）旨在打造一种信息共享平衡，即：将信息提供给保卫我们国家安全的须知者，让信息远离那些会给我们造成伤害的对象。尽管这两个优先点——共享和保护——通常看上去是相互排斥的，但事实上，这两点是相辅相成的。因此，本战略着重说明了为什么加强对机密和敏感信息的保护能够有助于打造信心和信任感，从而使此类信息能够在被授权使用者之间自由共享。

本战略确认，作为国家资产的关键信息必须同时加以适当的共享和保护。国土安全所面临的威胁一直在持续演变，因此按照计划，我们对此类信息加以使用和保护的政策也应当随之进行演变。这包括保护美国公民的隐私和个人信息，以及坚守我们对信息透明的承诺。这一战略明确阐明了一个立场，即美国公民的个人隐私、公民权利和公民自由必须，也将会受到保护。

我们国家的安全有赖于在正确的时间、向正确的人分享正确的信息。因此，我们将继续致力于维持一种适当环境，在这个环境中，**信息能够以负责、无缝和安全的方式进行共享**。在本战略的指导下，我们将继续为了保护国家安全和公民安全而恰当地运用关键信息。

摘要

美国的国家安全取决于在正确的时间、向正确的人分享正确信息的能力。这种信息共享义务需要联邦、州、地方、部落、区域、私人部门和外国合作伙伴之间进行持续且负责任的合作。在过去几年里，为了实现信息共享，我们已经成功简化了政策和流程，克服了文化障碍，以及更好地整合了信息系统。但是，当今的动态运营环境给我们带来了挑战，迫使我们继续完善信息共享和信息保护的流程与能力。尽管创新提高了我们的共享能力，但日益增加的共享也增加了缺陷漏洞出现的风险，因而需要进一步加强对信息的保护力度。对于如何进行有效开发、整合和实施，2012年的《信息共享与信息安全国家战略》提供了政策、流程、标准和技术方面的指导，致力于促进和实现一种安全且负责的信息共享。

面对这些挑战，我们必须拿出有战略性的应对方案，并且应当以三个核心原则为出发点：首先，在将信息视为国家资产方面，我们承认，各部门和机构已经获得了前所未有的能力，能够按照他们各自的任务和适用法律权限来收集、存储和使用信息；相应地，他们也有义务为了支持国家安全使命而提供信息。其次，信息共享和信息安全需要进行共同的风险管理。为了打造和维持共享所必需的信任，我们必须通力合作，找出并降低风险，而不是通过不彻底的共享来避免信息损失。再次，核心前提——“基于信息作出决策”构成了我们所有行动的基础，提醒我们，信息共享的首要目的就是为了能够更好地做出决策。本战略重点关注实现以下五个目标：

1、通过合作和责任制来推动多方集体行动。为了最好地实现共同愿景，我们需要团结合作，使用推动任务实施的治理模式，采纳能够建立信任度的通用流程，简化信息共享协议的开发过程，以及通过绩效管理、培训和激励来为各方的努力提供支持。

2、通过通用标准来完善信息的披露和获取。完善信息的披露和获取，需要制定关于向被获准个人提供信息的明确政策。信息披露和获取的安全性依赖于身份识别与认证、授权控制、数据标识、数据关联、通用信息共享标准，以及一个严格的流程，来确认和验证上述内容的使用。

3、通过服务共享和互操作性来优化任务的有效性。任务有效性的优化需要：共享服务、数据和网络的互操作性，以及获取效率的提高。

4、通过结构性的变革、政策和技术解决方案来加强对信息的保护。为了培养信任以及保护信息，政策和协调机构必须重点关注识别、预防、减少内部威胁和外部入侵，而各部门和各办事机构则需要提高数据层控制、自动化监控以及交叉分类解决方案的能力。

5、通过一致性和合规性来保护隐私权、公民权和公民的自由。维持公共信任不可缺少的要素就是提高一致性，藉此我们可以在政府间实现对隐私权、公民权和公民自由的保护，在信息共享操作开发中融入相应的保护措施，以及推广问责制和合规性机制。

共同签署本战略后，我们将把信息视为国家资产，向所有被授权的使用者进行信息去向追溯，为那些肩负保卫国家安全职责的人士提供力量。只有我们通力合作，以认真负责的态度朝着目标努力，才能为我们的国家创造应有的安全。

一、引言

为了防止美国领土上的恐怖主义行动，我们必须寻求情报部门、执法部门和国土安全部的全体配合。我们将继续整合、影响有能力共享机密信息的州及主要城市地区；建立一个全国范围的可疑活动报告框架；为我们的反恐信息系统实施一种综合方法，确保分析家、代理机构和有关职能人员能够在政府中获取所有相关的情报信息。通过向联邦、州和地方部门联网的方式，我们正在完善对信息的共享与合作，实现信息和资料的无缝交换，以及开展调查和合作相关事宜。

《国家安全战略》， 2010年5月

国家安全有赖于在正确的时间、向正确的人分享正确信息的能力。随着全球网络日新月异的发展，克服国家安全挑战——无论是来自外部还是内部——需要持续合作和信息共享。保护美国公众的使命需要各层级的协同合作，上至联邦和各州，下至地方、部落和区域。情报部门、国防部、外交部、国土安全部、执法部门和私营部门团体之间的合作是必不可少的。

（一）实施范围

在2010年《国家安全战略》基础上制定的2012年《信息共享与信息安全国家战略》（以下称为本“战略”），提供了政策、流程、标准和技术方面的指导，致力于促进和实现一种安全且负责的信息共享。

本战略并未明确定义具体哪一类或哪一种信息必须被共享；相反，本战略将信息共享和保护政策的重点转移到了定义支持有效决策的信息要求上。本战略概述了在现行法律和政策内，指导信息共享和保护的国家政策蓝图，不会取代《信息共享国家战略》（2007年），后者将继续提供政策框架以及指导众多以完善信息共享为目的的核心举措。本战略将继续突出强调在这一背景下对个人权利的适当

保护——此处所述个人权利主要指隐私权和公民自由。然而，各部门和机构必须始终坚持不渝地坚守其按照各自权限保护全体美国公民民主权利的职责

（二）实施愿景

对美国而言，最首要的就是高效、适当地进行信息共享以及信息保护，以保护美国民众和国家安全。本战略指出了一种发展方向，在法律或政策的约束下，随时随地向任意授权用户提供正确信息，来为国家安全决策提供支持，这种提供不存在技术上的限制瓶颈。此外，为保护此类信息，需要采取包括综合问责制在内的措施体系，以防止对信息的滥用。

（三）已取得的进展

尽管2012年的战略为未来设定了目标，但为满足《情报改革和防范恐怖主义法》（2004年）的制度要求，特别是在提高关于恐怖主义、国土安全和大规模杀伤性武器的信息整合方面，2007年的《信息共享国家战略》仍然将继续提供政策框架指导。此外，在政府、公众和私人部门之间进行及时、可用的双向信息流动方面，对于上述三种实体产生的数据，2007年的《信息共享国家战略》还突出强调了收集和报告的重要性。迄今为止，这些合作伙伴的不懈努力已经取得了显著的进展。

一是，建立了一个由州和地方政府所有、管理的国家网络中心，利用国家级可疑活动报告（SAR）措施（NSI）在各层政府之间共享恐怖主义信息，同时采取一贯政策保护个人隐私、公民权和公民自由。各网络中心、联邦调查局（FBI）的联合反恐工作组、战地和区域情报工作组、联邦、州及地方执法机构、高强度贩毒地区项目、区域信息共享系统中心、情报和犯罪分析单位（包括部落和非执法机关合作伙伴），通过网络中心联络官项目等措施，上述机构或组织之间正在开展着日益密切的合作。

二是，采用了国家信息交换模型（NIEM），通过构建数据交换通用方式，更好的实现信息共享。目前，许多联邦机构、州政府、私营部门组织和外国合作伙伴都在使用这一模型。此外，由于与多家标准开发机构（SDO）的合作，国家信息交换模型还产生了一个附带效益，推动了IT产业对这一信息交换模型的广泛使用。

三是，基于《网络空间可信身份国家战略》中联邦身份认证和访问管理（FICAM）框架，在各系统中对于用户身份认证和授权实施了统一的一致性计划。这是建立信息共享使用个人责任制和促进适当级别信息访问的关键一步。

四是，按照相应的任务权限和法律保护，访问跨部门、跨机构的多个数据库。举例来说，国家反恐中心（NCTC）的分析家现在就可以访问包含恐怖主义信息的30多个联邦局域网。这与911之前数据库以机构为中心的特征形成了鲜明对比。

五是，对于已知或可疑的国际恐怖主义者身份，在国家反恐中心开发了一个权威数据库。现在，来自国家反恐中心数据库的相关信息可以输出到联邦调查局的恐怖主义筛选中心数据库中。这个数据库也包括了国内已知或合理被怀疑为恐怖主义者的人员身份清单，形成了多重信息来源，并进行整合的信息清单。

最后，完善了促进各部门和机构与其他合作伙伴之间对话的沟通机制。举例来说，联邦调查局和国土安全部（DHS）在一年365天中，每天都会和十几个反恐组织举行三次秘密的视频会议。这些成果在适当时可以提供给联邦政府机构外的合作者。

通过这些根本性的努力，我们已经成功开始简化政策和流程，克服了文化障碍，完善了信息技术系统的互操作性，让关联信息共享成为可能。

二、现状

不断发展的信息技术，为信息共享利益相关方在识别和实施信息管理最佳实践做法方面带来了挑战。尽管创新使信息可以跨越司法、职能和组织的边界，畅通无阻地移动，但是越来越密集的信息共享也可能会造成漏洞，使我们面临信息的危害、爆炸、伪造和滥用。这些通常会在治理、信息管理和资源寻求方面带来更大的挑战。

国家安全面临的威胁仍然呈现多元化态势。我们所面临的威胁多种多样，例如恐怖主义者对美国国土和海外利益的攻击，信息系统内在的威胁与漏洞，核扩散，网络攻击，全球经济压力以及区域不稳定性等等。随着对手学会如何应对我们的安全措施，未来的威胁只可能会越来越大。这些威胁的广泛性和动态组合性表明，及时有效的信息共享和信息保护是必不可少的。

管理手段和政策的多样性带来了障碍。对于信息共享和信息安全保护，各部门和机构需要肩负起相应的法律责任，摈弃以往各自为政的做法和政策理念，从全政府的角度出发，同意参与到结构化的协作中来。更好的协调管理框架，为信息共享和信息安全保护提供政策和操作流程的制定机制，以使政策执行和管理手段实施更加高效和低成本。

信息共享的质量控制存在困难。与国家安全相关的信息可能不完整、模糊或不准确。因此，对于确保质量控制而言，在信息获取、访问、保留、复制、使用、管理、共享以及保护时，创建工具和技术，帮助利益相关方评估信息来源是十分必要的。

信息共享存在限制和约束。在共享敏感的操作信息、执法信息或个人身份识别信息方面，总是会存在着一些限制约束。此外，外国合作者、州政府及私营部门也可能会对其信息的使用或扩散加以限制。因此我们需要做的是，尊重这种现实的存在，提供一种负责的信息共享方式，如“标识”数据，对用户身份识别认证，以及确保网络安全等。这些努力对于此类信息的适当保护是十分关键的。

网络缺乏互通性为跨各部门信息共享形成了障碍。政策和技术之间的差异，妨碍了授权用户在不同网络访问关键资源和信息的能力。目前我们正在努力，希望能够实现“敏感但非机密”网络和机密网络的互通性，减少用户访问这两种网络承载信息的障碍，同时高度保护此类信息的安全。

日益增长的信息共享需求提高了数据关联和分析能力。将大量数据转化为可随时使用的信息或情报，仍然是一项长期面临的问题。但是，为了能够采用先进的分析学对信息进行加工，许多措施正在开发中，包括新工具、技术和相关培训。

提高效率是首要任务。在过去几年中，经济的衰退影响着每一个人，包括家庭主妇、商人和政府。因此必须在极其紧缩的预算环境下，以创新和灵活的方式来实现任务目标。

对信息实施适当保护。对共享信息进行适当保护的能力，与治理流程、访问控制、身份管理、审计能力以及网络互通性的成熟度存在着直接关系。这使我们在单个网络和系统内控制信息质量与访问，转向跨部门进行信息管理的共享。

三、原则

公民的想法、价值观、能量、创造性以及适应力，是美国最宝贵的资源。社会将向有所准备、时刻保持警惕并且鼓励积极参与的方向发展，其中公民是核心。此外，我们必须通过和私营部门、非政府组织、基金以及社区组织的战略合作来挖掘政府部门以外的创新潜力。这些合作伙伴对美国在本土和国际上成功施政十分关键，因此我们将会为他们提供支持，创造更多的协作机会，推动信息共享和公开透明。

《国家安全战略》， 2010年5月

为了完成本战略的愿景，需要以三个核心原则为基础开展努力：

（一）信息是国家的资产

各部门和机构已经获得了前所未有的能力，能够按照他们各自的任务和法律适用权限来收集、存储和使用信息；相应地，他们也有义务为了支持国家安全使命而向任意机构、部门或具备相关国家安全使命的合作伙伴提供信息，以及以合法方式管理此类信息和保护个人权利。这就需要信息安全保障、信息访问控制、管理政策及流程的不断成熟完善。

例如，信息访问，从以往限定在某个机构的内部网和应用系统，转向为用户提供一种基于政府业务领域的访问方法，通过信息安全保障和授权访问，实现跨部门的信息共享。

将信息作为一项国家资产进行管理的同时，还要求利益相关方保证政府、公众或私人机构对信息的及时获取，同时还要防止信息被无意或非授权使用。尽管信息拥有者对共享信息的准确度、特征及可获取性负有责任，但用来报告或制定决策的信息使用者，对信息的使用方式负有同样的责任和义务。总之，每位利益相关方所收集、分析和传播的信息都必须是可披露且可追溯的信息，必须遵守相关法律要求，并以政府的政策、标准和管理框架作为指导。

（二）加强信息共享的风险管理

信息共享和信息安全保障所需信任体系的建立，需要培养管理风险的能力，而不是如何规避风险。如果共享的方式不一致、分散独立，或仅以单独机构的角度出发予以管理，则会增加国家的安全风险。但是，不断完善政策和标准、加强警示宣传和综合培训，实施有效的治理以及完善问责制度，风险是可以降低的。政府业务领域级别上的绩效管理和合规性监察，会有助于治理、决策通报，以及强调负责任进行信息共享的重要性，这一文化氛围的培养。

信息的共享和保护不是相互排斥的。适当的信息共享和保护政策、规范及方式可以在实现恰当保密的同时提高透明度。为了实现信息共享的益处，利益相关方应在保护信息的流程中采取适当措施创建信任，从而减少和管理风险。随着信息共享使命紧迫性的提高，完善信息保护技术的互操作性需求也在增强。

（三）保障决策制定所需信息的可用性

充分知情的决策需要使用准确、相关联、及时的信息，以具备发现和检索的能力。同样，国家安全取决于让信息能够以一种受信方式（在特定任务背景下），

轻松地被联邦、州、地方、部落、区域、私营部门及外国合作伙伴所获取的能力。我们的目标是，通过对政策、指南、交换标准和通用框架的一致性应用，提高信息在操作中的有用性，同时始终坚持对个人隐私和个人权利的尊重。

最终，信息共享的价值需要按照其对决策的贡献来衡量。上述原则和下述目标将帮助我们实现一种环境——在这种环境中，决策是受信息所驱动的，从政策制定人员到联邦机构领导的每个层级上，都能够体现出我们的最佳评估。

四、目标

（一）加强协作和落实责任制来促进合作

1、完善治理，促进合作

政府的治理机构在设定行动优先级和制定决策方面起着关键的作用。在问题可能发生的最初阶段，需要明确各级政府的工作职责与需求，创建和谐的工作氛围，补充宪章内容来支持协作和强化政策的执行。此外，也允许通过白宫政策流程将问题上报。有效的治理结构能够更好的处理多种任务的复杂性，确认资源现状，缩减差距，最大程度地减少冗余，协调利益相关方的政策制定和执行。

2、增加对通用流程的使用

许多团体为了获取、访问、保留、制造、使用、管理、共享和保护信息而采取通用的流程。举例来说，国家网络中心和地方执法部门所使用的可疑活动报告流程，以及能够在全国范围内识别和报告各辖区可疑活动的技术，作为可疑活动报告信息共享的通用流程。类似可疑活动报告的通用流程，为各组织提供了一个可以复制、互通且受信的协议模板。在标准制定方面，随着任务需求的不断扩展，其内置的灵活性对于信息的及时发现、访问和交互，起到了很好的改善作用。同时，也使新合作伙伴能够更容易地融入现有信息流。对通用流程日益增多的使用，不仅为保护隐私、公民权和公民自由提供了机遇，还有利于加强信息保护核准措施的执行。

3、简化信息共享协议开发流程

为了保护国家安全而进行的信息共享，依赖于从众多政府机构、私营部门和外国合作伙伴获得信息的能力，而上述所有对象均有着不同的使命以及不同的信息收集和传播政策。因此，在进行跨部门合作的过程中，制定跨部门信息共享协议通常是十分关键的一步。但是，这一步所需要的时间往往会被拖延，因为基于不同使命、要求、限制以及信息获取、处理和使用的权限，政府部门通常会尽量满足双方均可以接受的要求和限制。创建一个以通用法律和满足政策合规性要求为基础的模板会简化这一流程，推动问题的尽快解决，促进与私营部门及外国合作伙伴的合作。

4、通过绩效管理、培训和激励措施推动发展

实现本战略的目标，需要制定一种为组织和个人绩效提供激励的管理方法。在对信息共享和保护的实施进度进行整体评估时，加入绩效管理方法后，部门和机构可以从中获益。利益相关方不仅应该衡量信息共享和保护流程中的进展（如可披露性、及时性、准确性、合规性和监督），还应衡量它们的整体效用（如共享信息在实现任务方面起到了怎样的作用）。经过有效的领导，绩效管理和衡量指标能够推动进度，激励人员满足较高的期望值及职业标准。通过培训和激励方式对员工进行的投资，从小团队扩展到整个组织，也会有助于培养一种重视信息共享和信息保护的文化氛围，

（二）采用通用标准来完善信息发现和获取的流程

1、为发现和获取信息制定明确的政策

信息共享的核心目的，就是让那些有合法需求的人能够及时地了解和获取特定信息。披露和获取是两个完全不同的概念：前者针对的是一个用户识别信息存在的能力，而后者是指一个用户检索出信息的能力。我们的国家安全需要按照现行法律和政策，将相关信息披露给适当的人员。披露和获取都需要清晰且一致的政策和标准，以及能够执行互通流程和技术的技术指导。

2、完善身份识别、鉴定和授权控制

信息披露需要对身份验证有一个标准化的方法，从而使参与实体对试图登陆系统的用户身份能够查证和信任。信息持有人通常会创建自有的验证服务，这为用户访问不同的系统或网络形成了障碍。使用受信互通的验证服务就能最大程度地减少所需身份验证的数量，驱逐不必要的匿名者，这样通过消除独立验证服务来提高验证的效率。

一旦查证了用户身份，身份属性就会帮助系统确定是否授权其访问信息。信息所有者和使用人都共同承担责任，使用标准流程、属性及“使用规则”，来支持验证和授权决策。此外，为了给决策提供信息，用户属性需要进行动态管理，为灵活更新和撤销用户访问做好准备。更大范围跨部门跨机构的政策和技术联盟，将可以实现互通能力，在确认用户合法性的过程中建立保守秘密和信任感，同时对任务的相关信息提供访问权。

3、促进数据级别的贴标

大多数信息授权模型限定在网络或应用层级上进行定义和实施访问控制，而不是在数据层级上，对具体的信息资源描述其内在特征。随着网络整合和共享服务的出现，访问控制必须通过数据“贴标”的方式来实现。贴标是一种将标准化的属性信息，即标签，附加在一条数据上，从而对数据进行描述的方法。通过贴标，用户可以了解数据的简要描述信息，从而直接获取具体数据，这种方式提高了人工的数据发现和访问能力。此外，数据贴标也能根据任务的关联性做出自动化访问的决策。将使用者属性与对应的信息属性进行搭配后，可以提高任务特定信息的自动交付，同时避免将该信息提供给不恰当的接收者。此外，数据贴标还有助于数据的记录管理，及时响应查询，整合隐私保护，修复错误的数据披露并进行修改。

4、提高数据的关联性

将不同部门和机构数据库的相关信息联系起来，对威胁识别和降低攻击的发生，将有力地缩小这两种方式的差别。数据关联和高级分析，以及整合信息的共享和信息保护，将使用户可以跨越多个机构查询到最权威、最新的资讯。这种能力可以支持分析家发现不同人群、地点、事物和特征的关联关系，如果不具备这种能力，这些关联关系往往并不明显。为了提升这种能力以及考虑到信息量的增加，利益相关方需要开放其拥有的信息，从而使分析家可以在众多信息资源进行

检索。此外，数据资源还需具备自动关联关系建立，以及当与任务相关的信息可以访问时，向用户自动推送提示信息的能力。尽管在一些受限的情况中，目前的技术需要集中信息存储，但分散处理方法能够允许信息所有者按照需求来维护和更新信息。这种方式能够增加信息共享的速度，实现更高级别的信息保真度。此外，数据关联的建立也需要对信息的真实性和适用性进行验证。

5、推动信息共享标准的使用

跨政府部门业务领域的数据发现和访问，保障了信息共享标准的使用。通过对现有标准的再次使用，利益相关方可以共享一项新标准在审核和执行中投资的时间、资源和经验。因此，满足任务需求的能力可以变得更快捷、充分和有效，无需为了某一次的使用，而特定编写客户解决方案或标准。为谨慎地实现信息共享，可以自愿使用联邦政策中现行的标准，其中，政府使用由标准开发机构创建的标准。标准开发机构通常包括政府、行业和国际成员。基于这种方法，我们的第一个目标是采纳现有标准满足任务需求，当无法满足时，再由标准开发机构制定新的标准来填补这一缺口。

6、推动跨政府部门标准认证和保持一致性

鉴于政府、私营部门和国际团体之间存在着大量标准，决策者和使用者需要决定哪个标准最能满足需求，同时还能支持与其他合作者之间的互通性。因此，对于信息共享技术方案的互操作性，需要建立一个流程来验证。相应地，这一做法也会帮助决策者选择最适当的标准，并且政府的行为向行业发送出明确信号，在进行产品和工具开发，提升互操作性以及更大范围满足任务的需求，企业如何选择标准。

（三）共享服务和改善互操作性来提高效率

1、服务共享

在政府中，各部门和机构已经开始使用共享计算模型——“云计算”。在这种模型中，数据中心是统一的，计算机基础设施被用于提供共享服务。通用基础设施上的主机系统和应用分配了工作负担，降低了对计算性能的要求，并且减少了总成本。将来，除共享计算能力以外，可能会通过提供其他能力带来额外的改进，例如共享应用和共享信息服务。因此，各部门和机构可以继续使用现有性能，

将目光关注与服务和技术的开发上，来更好的满足部门职能。特别地，性能共享将使部门和机构为特定的终端用户提供有针对性的服务，而不是为所有用户尝试性的提供所需全部性能。这一方法的预期优势包括简化成本，提高效率，以及减少个性化的界面和所需标准的数量。

2、提升数据、服务和网络的互操作性

尽管共享服务模型带来了显著的改善，但也不能保障互操作性或改善信息共享。在各种涉密和非涉密的网络中，仍然存在不同程度跨网部署的数据、服务和系统，部门和机构面临着挑战，而信息技术开发通常不能将互操作性放在足够的优先级上。通过在信息技术方案的设计阶段进行规划和优先排序，各部门和机构在满足单个任务需要的同时，进而实现互操作性所带来的整体效益。提高互操作性，开放服务及信息的共享，能够帮助政府更好的履行职能，最大程度地降低IT项目的复杂度，减少重复建设以及满足持续维护的需求。

3、推广政府采购

对于互操作性技术方案和共享服务的部署，使用标准化的政府采购方式是十分必要的。随着政府与其他组织开展合作，对最佳解决方案的识别和重用，以及多任务标准化技术的开发，我们整合系统和共享信息的能力正在变得更强大、更具有适应性。

此外，鼓励利益相关方和行业共同配合，在信息共享和信息保护标准方面，开发和获取相关工具及技术。联邦政府采购政策，应当促进和奖励各部门和机构间的合作，以推动对现有服务的再次使用。同时，在全政府范围，鼓励制定政府采购的优先级顺序。根据政府采购要求，不仅要采用具有互操作性技术的产品和服务，还要降低采购和政采成本，以减少部门和机构日益增长的开销。

（四）结构性改革加强对信息的保护

1、结构性改革和政策制定

最近的信息失窃和泄漏，凸显了在敏感及机密信息保护方面的漏洞。但是，持续进行的结构性改革和政策标准化将会加强监管，规范最佳安全实践办法。

信息的非授权披露和滥用风险来自内部威胁和外部入侵，改革必须同时针对这两点来进行。监管网络、检测反常行为，从而识别内在威胁和外部入侵，实施

和巩固这些方面的政策和流程，将加强保护信息的能力。现有的协调机构仍然重点关注信息保护和开展以下工作：开发有效的技术政策和标准来协调政府范围的实施，开展独立的合规性评估，以及落实高级官员的责任制。来自多网络多领域的反间谍、安全、信息保障和人力资源等要素信息的适度实时汇总，使得主管当局能够有效地减少并解决安全泄漏问题。类似地，基于全局性地理解各项应用和服务在跨网络、跨安全领域中的部署情况，整合全政府范围内的IT能力，来监测网络的健康状态和尝试性的恶意访问。此外，政策和流程也应该解决信息的意外泄漏问题。预防、监测和应急政策，结合适当的支持性技术，对于机密信息的共享，能够在合作者之间提供安全保障和培育信任。

2、加强数据层控制、监控自动化以及制定交叉分类的解决方案

科技在加强信息保护能力方面也起着重要作用。随着科技发展，我们需要通过使用具有互操作性的应用，将控制从网络层转移到数据层。越来越细微的安全控制将提升对信息的访问能力（无论信息流向何处），增强对信息的非授权披露、传播、访问及修改的防治。持续的监控自动化，实施适当的隐私保护，可以支持共享风险管理，实现对现有或潜在风险的实时监控。

在过去，对信息保护的关注主要局限在特定类型的系统和网络上。但是，各部门和机构通常会在不考虑类别的情况下，在各系统间寻找可以安全共享信息的方式。科技、性能和服务（如共享计算等）进一步加速了交叉分类实施共享的需求。因此，我们需要一些能够支持此类关键新兴需求的技术、标准和通用流程。

（五）保护隐私权、公民权和公民自由

1、在政府范围实施连贯、持续性的保护政策

对维持公众信任度而言，加强隐私权、公民权和公民自由的保护是不可或缺的，这是我们进行信息共享和信息保护的基石。各部门和机构需要采用一种连贯一致的方法来保护最基本的隐私权、公民权和公民自由，同时按照现有法律和政策规定留出一定的弹性空间，这样可以调整治理结构和现有流程，为共享信息实施适当保护进行持续性的改善和建立必要的政策指导，如《信息共享环境隐私准则》。联邦和非联邦合作伙伴之间共享信息时，在法律法规和政策条款的要求下，培养一种综合有效的方法对隐私权、公民权及公民自由的保护进行定义和实施，因此，保护国家安全和保护个人权利同等重要。

2、在信息共享流程中建立保护措施

保护隐私权、公民权和公民自由并不仅仅是法律顾问和专家所需要考虑的领域。对于信息使用方面的法律和政策控制，在政策制定过程中予以执行，这一做法同样适用于科技的运用过程。这一点表明，项目经理、系统建筑师和开发者、信息保障人员以及其他参与项目和系统设计的人必须予以参与和配合。在新行动的计划早期（或现有系统和流程的重新设计阶段）就将隐私权、公民权和公民自由作为一个问题来解决，会使这些信息的保护能够在全政府范围内被考虑、管理和监控。

3、推广问责制和合规性机制

通过加强监管、绩效管理和落实责任制等方面的机制来确保合规性，是非常关键的。目前，各部门和机构利用适当的合规文件和绩效管理技术，来监控和报告，实现对隐私权、公民权和公民自由的保护。监控和问责制的合规性能够帮助任务合作伙伴识别和解决其中的漏洞，并且在验证时能够使任务合作伙伴主动、系统地对个人权利的保护进行完善。随着我们在全政府范围内使用这个方法，必须对保护措施进行持续的巩固和评估，包括对访问和使用控制的监控、对审计和实用信息的分析，以及对系统合规性的定期检查。

隐私权、公民权、公民自由的绩效管理和合规性，必须随着信息共享需求和信息共享方式的变化发生演变。随着发展，这种跨政府部门的模式应该包括，使用技术手段审查和强化对隐私权、公民权、公民自由的保护力度。

（六）下一步发展目标

正如《国家安全战略》中所述，“开展跨政府部门的合作，必须成为我们的行动指南。”完善信息共享和信息保护，以增强国家的安全保障能力，本战略是协调各方合作的指导性纲领。政府的决策制定基于大量的关联信息，在尊重法律和政策对信息使用的各种限制要求时，相应地对信息、来源和收集方法进行适当保护。本战略的顺利实施，取决于多方的合作以便在共享和保护之间达到平衡，基于以往实施的经验，继续培育信息共享的环境，不断发展成熟。

为了完成本战略的目标，实现愿景，需要提供一种协调且可持续的方法，因此需要制定一份整体的执行方案。该方案将重点关注实现五年期内的优先目标和排位靠前的利益相关方活动，使用绩效衡量和里程碑管理战略实施进度，确定牵头执行部门。执行方案将整合年度纲领和实施指南，与联邦预算周期同步，从而

允许按照年度绩效评估、优先级的变动和资源分配，来调整行动和交付成果。实施方案需要在白宫的带领下，所有涉及国家安全的部门参与OMB对战略资源的分配过程，由适当的部门、执行机构根据任务的关联性和现行职权进行管理。

1、优先发展目标

前五个优先目标。在实现本战略信息共享和信息保护的目标过程中，以下目标是最重要的五个管理目标：

1、梳理信息共享和保护的治理结构，来形成有效的决策制定、实施绩效、责任制落实和战略目标的执行。

2、为信息共享和保护协议制定纲要，解决共性要求，包括隐私权、公民权和公民自由，同时保持政策弹性，满足政府部门职能个性化需求。

3、采用元数据标准来推动跨网络和安全领域的数据发现、访问、关联，以及监控。

4、在所有安全领域实施联邦身份认证和访问管理控制。

5、实施可灵活调整的政策、流程和控制手段；对资产、漏洞和威胁，提供可以及时审计的能力；对于内部威胁，采用防御、监测和干扰的手段，具体有程序、流程和相关技术；共享风险管理，从而加强对非机密和机密信息的保护。

2、其他目标

以下目标是各部门、机构和其他利益相关方为了促进本战略目标的实现，而需要开展的额外优先活动：

1、为了实现数据、服务和网络互操作性，定义、采纳的基准能力和通用要求。

2、为了推广一致、弹性且受信的流程，定做的通用课程，用来对利益相关方进行信息共享、信息保护和处理进行培训。

3、为了支持基于政策的信息自动化发现和访问控制，定义、执行通用的流程与标准。

4、建立与私营部门合作者的信息共享流程，以及针对特定部门的协议，提升信息质量和及时性，确保国家基础设施的安全。

5、开发一个参考结构，用于在数据发现和不同数据集间建立关联关系，提供一致的方法。

6、在不同利益相关方之间执行联邦IT共享服务战略的建议和活动，为共享服务的采纳创造便利。

7、在不同部门和机构、标准实体及供应商之间,完善标标准认证和一致性的流程，推动标准化的信息获取，促进产品和服务的互操作性。

8、遵守对现有跨机构的流程，协调与外国合作伙伴的信息共享活动，采纳和应用必要的纲领，遵守法规和总统政策，确保信息共享和保护时的一致性。

9、在各层级政府，为信息请求、警告、预警和通知建立一个通用的流程，从而能够及时地接收和发布信息，并做出适当回馈。

10、在国家网络中心和联邦政府部门中，完成国家级可疑活动报告措施项目的实施，同时将培训扩展到执法部门以外的公共安全机构。

11、对于威胁相关信息的接收、分析与整合，在州和地方政府范围内，通过跨政府网络，实现四大关键业务能力，四大必备能力以及上述优先目标，来有效的执行政府权威性职能。

贯穿于整个政府的国家安全利益相关方，在我们共同原则的指导下，现在可以一起为了实现本战略目标而努力，完成上述优先目标以及打造对本战略的执行方案。共同签署本战略后，我们将把信息视为国家资产，向所有被授权的使用者进行披露和追溯信息去向，为那些肩负保卫国家安全职责的人士提供所有必要的信息，推动保家卫国决策的出台。只有我们通力合作，以认真负责的态度朝着目标努力，才能为我们的国家创造应有的安全。