

第 21 号总统政策指令

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Presidential Policy Directive 21/PPD-21		
原文作者	白宫新闻秘书办公室	原文发布日期	2013 年 2 月 12 日
作者简介	<p>白宫新闻秘书办公室负责收集信息并向三个主要群体传播信息：总统、白宫的工作人员、媒体。该办公室是由白宫新闻秘书领导，是白宫办公室的一部分，也是总统行政办公室的下属部门。</p> <p>http://en.wikipedia.org/wiki/White_House_Office_of_the_Press_Secretary</p>		
原文发布单位	白宫新闻秘书办公室		
原文出处	http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	<p>本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。</p> <p>本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。</p> <p>译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。</p> <p>本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全</p>		

	部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。
--	---

白宫

新闻秘书办公室

直到总统 2013 年 2 月 12 日的国情咨文发布前禁止传播**2013 年 2 月 12 日****第 21 号总统政策指令/PPD-21**

主题：关键基础设施的安全和恢复能力的总统政策指令（PPD）旨在促进民族团结，共同加强和维护关键基础设施的安全、运作和恢复能力。

简介

国家的关键基础设施提供了支撑美国社会的基本服务。主动和协调的各方工作对加强和维护关键基础设施（包括资产、网络 and 系统）的安全、运作和恢复能力是必要的；对公众信心和国家安全、繁荣和福祉也是至关重要的。

国家的关键基础设施呈现多样化和复杂化。它包括分布式网络，不同的组织结构和经营模式（包括跨国所有权），物理空间和网络空间中相互依存的功能和系统，涉及多层机构、职责和规定的治理结构。关键基础设施的所有者和经营者具备得天独厚的优势来管理业务及资产风险，并确定有效的策略提高基础设施的安全性和恢复能力。

关键基础设施必须是安全的，并能够承受风险并迅速从所有风险中恢复过来。为了实现这一点，需要国家防御系统（包括预防、保护、减灾、响应和恢复）的协作。

该指令规定了关键基础设施安全性和恢复能力的国策。这个任务是所有联邦、州、地方、部落和领土（SLTT）的机构、关键基础设施的公共和私营所有者和经营者（以下简称为“关键基础设施的所有者和经营者”）的共同责任。此指令还细化和明确了整个联邦政府与关键基础设施相关的功能、角色和责任，并致力于提高整体的协调和合作。联邦政府也有责任加强自身关键基础设施的安全性和恢复能力，以便实现国家基本功能的连续性；并有效地与关键基础设施的所有者和经营者合作，以便增强关键基础设施的安全性和恢复能力。

政策

加强关键基础设施的安全性和恢复能力以应对物理和网络威胁，这是美国的一项国策。考虑到所有风险都可能对国家安全、经济稳定、公众健康和安全等产生不利影响，联邦政府应与关键基础设施的所有者和经营者/SLTT 机构合作，采取主动措施，以管理风险、加强国家关键基础设施安全和恢复能力。这些努力应寻求减少漏洞、最大限度地减少影响、识别并中断威胁、加速关键基础设施相关的响应和恢复能力。

联邦政府也应与国际伙伴合作，加强对国内关键基础设施和美国依赖的境外关键基础设施的安全和恢复能力。

美国应以综合全面的方式解决关键基础设施的安全和恢复能力问题，以反映基础设施的相互联系和相互依赖性。该指令还确定了能源和通信系统，这是因为这些系统对所有关键基础设施部门提供不可替代的功能。

三大战略举措应该能够帮助联邦政府加强关键基础设施的安全性和恢复能力：

- 1) 确定并阐明整个联邦政府的职能关系，以促进民族团结，共同加强关键基础设施的安全性和恢复能力；
- 2) 通过确定对联邦政府的数据和系统要求，以促进有效的信息交流；
- 3) 实施整合和分析功能，以将关键基础设施的规划和运营决策告知相关机构。

所有联邦部门和机构的负责人应负责各自内部关键基础设施（支撑主要任务基本功能）的识别、优先级、评估、修复和安全。这些基础设施应在《国家连续性运行政策》的计划和要求中予以说明。

联邦部门和机构应在遵守适用法律、总统指令和联邦法规（其中包括保护个人隐私、公民权利和公民自由的法律）的情况下执行该指令。此外，联邦部门和机构应当根据适用的法律和政策保护所有执行该指令的信息。

角色和职责

有效地执行该指令需要各部门和机构根据国土安全部长的战略指导团结起来。国家努力必须包括特定行业机构（SSA）的专业知识和日常参与；其他联邦部门和机构的专业能力或支持；与关键基础设施所有者和经营者/SLTT 机构的大力协作。虽然该指令中确定的角色和

职责都是针对联邦部门和机构的，但是与关键基础设施所有者和经营者/SLTT 机构的有效合作对加强国家关键基础设施的安全和恢复能力是必须的。

国土安全部长

国土安全部长应提供战略指导，促进民族团结，协调整个联邦政府的工作以促进国家关键基础设施的安全和恢复能力。在《2002 年国土安全法》中，国土安全部长评估了保护关键基础设施的国家能力、机会和挑战；分析了关键基础设施的威胁、漏洞、以及一切危害的潜在后果；确定了所有公私关键基础设施部门有效参与所必需的安全和恢复能力；制定了国家计划和指标，以便与 SSA 和其他关键基础设施合作伙伴进行协调；协调联邦跨部门的安全和恢复活动；识别并分析了关键基础设施部门之间的重要的相互依存关系；并报告了增强关键基础设施安全和恢复能力的国家工作的有效性。

国土安全部长的其他角色和职责包括：

- 1) 考虑到物理和网络威胁，与 SSA 以及其他联邦部门和机构协作确定并优先处理关键基础设施的漏洞和后果；
- 2) 维护国家关键基础设施中心的安全，这些中心应提供态势感知能力，其中包括新趋势、迫在眉睫的威胁、可能影响关键基础设施的事件的现状等信息；
- 3) 与 SSA 以及其他联邦部门和机构协作，向关键基础设施所有者和经营者提供分析、专业知识及其他技术支持；促进信息和情报的交流，以加强关键基础设施的安全和恢复能力；
- 4) 与 SSA、SLTT、关键基础设施所有者和经营者协作，对国家关键基础设施漏洞进行全面评估；
- 5) 根据相关法律，协调联邦政府对关键基础设施的重大网络或物理事件进行响应；
- 6) 支持司法部长和执法机构调查针对关键基础设施的威胁和攻击；
- 7) 利用 SSA 以及其他适当的联邦部门和机构的专业知识，使用商业卫星和机载系统、其他部门和机构的现有能力，对关键基础设施绘制地理空间地图、摄像、分析和分类；
- 8) 根据法律要求，对国家关键基础设施的工作状况进行年度报告。

特定行业机构

每个关键基础设施行业都有独特的特征、经营模式和风险状况，这些受益于具有对机构知识和专业知识的特定行业机构（SSA）。SSA 应了解特定联邦部门和机构的现有法定或监管机构，并充分利用现有行业熟悉度和关系。SSA 应对其各自行业履行下列职责：

- 1) 参与国家加强关键基础设施安全和恢复能力的工作，与国土安全部（DHS）及其他相关联邦部门和机构、关键基础设施的所有者和运营者协作，在适当情况下与独立的监管机构、SLTT 机构合作以执行该指令；
- 2) 充当特定部门行动的动态和协调接口；
- 3) 根据法定权限和其他适当的政策、指令或法规执行事件管理职责；
- 4) 提供、支持或推动该部门的技术援助和咨询，以确定漏洞并帮助缓解事故；
- 5) 根据国土安全部长的一切，提供具体行业的重要基础设施的年度信息。

其他联邦机构的职责

下列部门和机构对关键基础设施的安全和恢复能力有专门的支持功能，这些功能应与其他联邦部门和机构以及独立监管机构实施。

- 1) 国务院与国土安全部、SSA 以及其他联邦部门和机构进行协调，与外国政府和国际组织协作，以加强美国境外的国家关键基础设施的安全和恢复能力，促进最佳方法和经验教训的相互交流，以促进国家赖以生存的关键基础设施的安全和恢复能力的增强。
- 2) 司法部（DOJ），包括联邦调查局（FBI），应指导关键基础设施部门的反恐和反情报调查及相关执法活动。司法部应该调查、阻断、起诉或减少对国家关键基础设施的外国情报、恐怖主义和其他威胁，以及实际或企图的攻击。联邦调查局还应执行网络威胁信息的国内收集、分析和传播，并负责国家网络调查联合特遣部队（NCIJTF）的活动。NCIJTF 是一个多机构国家联络点，负责协调、整合和共享网络威胁调查相关的信息。其成员来自国土安全部、情报机构（IC）、国防部（DOD）和其他机构。司法部长和国土安全部长应合作履行各自的关键基础设施职责。
- 3) 内政部应与政府部门的 SSA 合作，以识别、优先处理并协调国家遗迹和图标的安全和恢复能力，并采取措施降低这些重要资产的风险，同时促进它们的使用。

- 4) 商务部 (DOC) 应与国土安全部及其他相关联邦部门和机构, 私营部门, 研究、学术和政府机构协作, 以提高基于网络的系统的技术和工具的安全性, 促进关键基础设施措施的开发, 适时推出工业产品、材料和服务, 以满足国家安全要求。
- 5) 国家情报总监 (DNI) 为首的情报机构 (IC) 应采用适用权力和协调机制, 以提供涉及关键基础设施的威胁情报评估、协调敏感或专有信息。此外, 维护国家安全系统的信息安全政策、指令、标准以及准则受总统和适用法律的监督, 并由各机构的负责人行使国家安全系统权力。
- 6) 总务管理局应与国防部、国土安全部等部门和机构协商, 以提供或支持关键基础设施系统的政府合同, 并确保这些合同包括关键基础设施的安全性和恢复能力的审计权。
- 7) 核管理委员会 (NRC) 监督执照者对用于研究、测试和培训的商业核电反应堆和非动力核反应堆; 用于医学、工业和学术环境的核材料; 核燃料制造; 核材料和核废料的运输、贮存和处置的保护。核管理委员会在可能的范围内与国土安全部、司法部、能源部、环境保护署、其他联邦部门和机构合作, 以加强关键基础设施的安全性和恢复能力。
- 8) 在法律允许的范围内, 联邦通信委员会行使其权力和专业知识, 与国土安全部、国务院、其他联邦部门和机构、SSA 在以下方面合作: (1) 确定和优先处理通信基础设施; (2) 确定通信部门的漏洞, 并与业界及其他利益相关者解决这些漏洞; (3) 与利益相关者(包括工业、外国政府和国际组织) 合作, 以增加通信行业关键基础设施的安全性和恢复能力, 促进最佳措施的制定和实施。
- 9) 联邦部门和机构应当向国土安全部长和必要的国家关键基础设施中心提供及时的信息, 支持跨部门分析, 并提高对关键基础设施的态势感知能力。

三大战略举措

- 1) 细化并阐明整个联邦政府的功能关系, 以促进国家的统一举措, 加强关键基础设施的安全和恢复能力。

能够加强关键基础设施的安全和恢复能力的有效国家举措必须由国家计划所指导, 国家计划能够识别角色和责任, 并能够获得 SSA、其他联邦部门和机构、SLTT 机构、关键基础设施的所有者和运营者的专业知识、经验、能力和职责的支持。

在过去的 10 年中, 新的方案和举措相继设立, 以解决特定的基础设施问题, 而且重点

已经转移和扩展。因此，涉及关键基础设施安全和恢复能力的联邦职能应加以明确和细化，以建立反映这方面的知识演变的基准功能，定义相关的联邦计划功能，促进联邦政府、关键基础设施的所有者和运营者以及 SLTT 机构之间的合作和信息交流。

作为这种细化结构的一部分，国土安全部应指挥两个国家关键基础设施中心：一个是物理基础设施中心，另一个是网络基础设施中心。两个中心应协同运作，并作为关键基础设施合作伙伴的联络点，获得态势感知和综合、可操作的信息，以保护关键基础设施的物理和网络领域。正如关键基础设施的物理和网络元素有着千丝万缕的联系，安全漏洞也是。因此，集成和分析功能（在战略举措 3 中进一步讨论）应由这两个国家中心共同实施。

这些国家中心的成功，包括整合和分析功能，依赖于它们从 SSA、其他联邦部门和机构、关键基础设施的所有者和运营者以及 SLTT 机构接收的信息和情报的质量和及时性。

这些国家中心不得妨碍联邦部门和机构负责人执行国防、犯罪、反间谍、反恐、或者侦查活动职责的能力。

2) 为联邦政府确定基准数据和系统要求，促进有效的信息交流。

安全、运作良好和具备恢复能力的关键基础设施需要各级政府和关键基础设施所有者和运营者之间的高效信息（包括情报）交流。这必须便于威胁和漏洞信息、以及促进态势感知能力开发的信息的及时交流。我们的目标是在主要系统发生破坏时，通过确定数据、信息格式和访问性、系统互操作性、冗余系统和备用功能的要求来实现高效的信息交流。

政府内部以及与私营部门之间的更多的信息共享能够而且必须在尊重隐私和公民自由的前提下进行。联邦部门和机构应确保所有现有的隐私方针、政策和程序的实施遵守法律和政策，高级机构官员应管理和监督信息共享过程中的隐私问题。

3) 实施整合和分析功能，告知涉及关键基础设施的规划和运营决策。

第三个战略举措基于前两个，并呼吁对关键基础设施的整合和分析功能，其中包括对事故、威胁和新风险的运作和战略分析。这应由举措 1 确定的两个国家中心共同实施，应包括漏洞、威胁及后果信息的整理、评估和集成，以便：

- a. 有助于优先处理和管理关键基础设施的风险；
- b. 预测相互依赖性和级联影响；
- c. 在事件前、中、后提出关键基础设施的安全和恢复能力的措施；
- d. 支持关键基础设施有关的事件管理和恢复工作。

此功能不得复制情报机构或国家反恐中心的分析功能，也不得涉及情报收集活动。但是，获得相关情报或信息的情报机构、国防部、司法部、国土安全部、其他联邦部门和机构应向国家中心提供相关的、及时的、适当的国家关键基础设施信息。此功能也将使用其他国家基础设施合作伙伴提供的信息，包括 SLTT 和非政府分析机构。

最后，整合和分析功能必须支持国土安全部的维护和分享功能，并作为一个普通的联邦服务近乎实时的态势感知能力，其中包括可能影响关键基础设施的迫在眉睫的威胁、显著趋势、事件认知的可操作的信息。

创新与研发

国土安全部长应与科学和技术政策办公室（OSTP）、SSA、DOC 和其他联邦部门和机构协调，提供信息来支持联邦和联邦资助的旨在加强关键基础设施的安全和恢复能力的研发活动，包括：

- 1) 促进关键基础设施的安全和恢复能力设计、更安全网络技术的研发；
- 2) 加强建模能力，以确定事件或威胁情景对关键基础设施的潜在影响，以及对其他行业的连锁效应；
- 3) 制定举措，以激励网络安全投资和关键基础设施设计功能（加强面对各种灾害的安全性和应变能力）的采用；
- 4) 支持国土安全部部长签发的战略指导。

该指令的执行

作为执行该指令的一部分，国土安全部长应采取以下措施。

- 1) 关键基础设施安全和恢复能力的功能关系。该指令签发之日起的 120 天内，国土安全部长应制定国土安全部和整个联邦政府的关键基础设施安全和恢复能力功能关系的指南。这应该包括这两个国家关键基础设施中心的角色和职能，并对分析和整合功能进行讨论。完成后，它应该作为关键基础设施所有者和运营者及 SLTT 机构的路线图，以指导联邦政府物理和网络威胁的职能和主要联络点。国土安全部长应协调 SAA 及其他相关联邦部门和机构在这方面的运作。国土安全部长应通过总统国土安全及反恐助理向总统提交该指南。
- 2) 评估现有公私合作模式。该指令签发之日起的 150 天内，国土安全部长应与 SSA、其他相关联邦部门和机构、SLTT 机构、关键基础设施所有者和运营者协调，对现行的公私伙伴关系模式进行分析，并对物理和网络空间的有效合作提出建议。评估应考虑简化协作和信息交流的流程，并尽量减少重复工作。此外，分析应考虑模式的灵活性和适应性，以满足不同行业的特殊需求；同时向联邦政府提供针对性的、有纪律和有效的方法，以便与关键基础设施所有者和运营者、SLTT 政府进行协调。该评估将提供加强伙伴关系（国家安全委员会系统指令确定的）的建议。

- 3) 为联邦政府确定基准数据和系统要求,从而实现高效的信息交流。该指令签发之日起的 180 天内,国土安全部长应与 SSA 及其他联邦部门和机构协调,召集一个专家小组,以确定基准数据和系统规定,促进加强关键基础设施的安全性和恢复能力的信息和情报的高效交流。专家应包括定期获取关键基础设施安全性和恢复能力信息的机构代表;确定和管理用于交换信息的技术系统的和人士;负责信息交换的安全的人士。与关键基础设施合作伙伴的互操作性;识别主要联邦、SLTT 和私营部门机构的关键数据和信息需求;数据的可用性、可访问性和格式; 交换各类信息的能力;将使用的系统的安全性;个人隐私和公民自由应得到适当的保护。该分析应提供数据共享和系统互操作性的基准要求,以便数据和信息的及时交流,以确保关键基础设施的安全和恢复能力。国土安全部长应通过总统国土安全及反恐助理向总统提交该分析。
- 4) 关键基础设施态势感知能力的开发。该指令签发之日起的 240 天内,国土安全部长应展示对关键基础设施近乎实时的态势感知能力,其中包括威胁、各种灾害信息以及漏洞;提供关键基础设施的状态和潜在的连锁效应;支持决策制定;传播可能拯救或维持生命,减轻损害,或减少在整个事件中关键基础设施能力进一步退化的关键信息。这种能力应该是具备的,并覆盖关键基础设施的物理和网络元素,使必要的信息整合成为可能。
- 5) 更新国家基础设施保护计划。该指令签发之日起的 240 天内,国土安全部长应通过总统国土安全及反恐助理向总统提交国家基础设施保护计划的更新,以解决该指令的实施,应对《2002 年国土安全法案》修订本的第 II 条的要求,并符合第 8 号总统政策指令提出的国家防备目标和系统要求。该计划应包括用来加强关键基础设施的安全和恢复能力的风险管理框架的识别;优先处理关键基础设施的方法;联邦政府内部用于同步通信和行动的协议;用来衡量国家管理和减少关键基础设施风险的能力的指标和分析过程。更新后的计划还应当体现国土安全部内部和整个联邦政府的职能关系,以及公私合作模式的更新。最后,该计划应考虑对部门对能源和通信系统的依赖,确定事件前措施、缓解措施或替代功能。国土安全部长应与 SSA、其他相关联邦部门和机构、SLTT 机构、关键基础设施所有者和运营者协调这方面的工作。
- 6) 国家关键基础设施安全性和恢复能力研发计划。该指令签发之日起的两年内,国土

安全部长应与 OSTP、SSA、DOC 及其他联邦部门和机构协调；应通过总统国土安全及反恐助理向总统提交国家关键基础设施安全性和恢复能力研发计划；该计划要考虑到不断变化的威胁环境、年度指标以及其他相关信息，以确定优先事项，并指导研发需求和投资。该计划自提交之日起每 4 年发布一次，而且可以按照需要临时更新。

该指令实施的政策协调、争议解决及定期审核应该按照第 1 号总统政策指令进行，包括使用由国家安全参谋部协调的跨机构政策委员会。

该指令中的任何条款都不会改变、取代或阻碍联邦部门和机构（包括独立的监管机构）按照适用的法律及其他总统指示和指令（包括但不限于对关键基础设施的规定）履行其职能和职责的权力。

该指令撤销了 2003 年 12 月 17 日发布的第 7 号国土安全总统指令/HSPD-7，即《关键基础设施的识别、优先级和保护》。根据 HSPD-7 制定的计划将一直有效，直至被明确撤销或取代。

指定的关键基础设施部门和特定行业机构

该指令确定了 16 个关键基础设施部门，并指定了相关的联邦 SSA。在某些情况下，将与 SSA 共享职责的部门指定为 co-SSA。国土安全部长应定期评估需要；批准关键基础设施部门的变化；并在改变关键基础设施部门或指定的 SSA 之前与总统国土安全及反恐助理协商。行业和 SSA 如下：

化学：

SSA：国土安全部

商业设施：

SSA：国土安全部

通讯：

SSA：国土安全部

关键的制造业：

SSA：国土安全部

水坝：

SSA：国土安全部

国防工业基地：

SSA：国防部

应急服务：

SSA：国土安全部

能源：

SSA：能源部

金融服务：

SSA：财政部部

粮食和农业：

Co-SSA：美国农业部，卫生和公众服务部

政府设施：

Co-SSA：国土安全部，总务管理局

医疗保健和公共卫生：

SSA：卫生和公众服务部

信息技术：

SSA：国土安全部

核反应堆、材料和废物：

SSA：国土安全部

运输系统：

Co-SSA：国土安全部，运输部

水与废水系统：

SSA：环境保护局

定义

在本指令中：

“一切危害”是指自然或人为的威胁或事故，这些威胁或事故使得人们采取行动来保护

生命、财产、环境、公共健康或安全，并最大限度地减少对政府、社会或经济活动的破坏。这包括自然灾害、网络事件、工业事故、传染病、恐怖活动、破坏、破坏性的犯罪活动、针对关键基础设施的破坏性犯罪活动。

“协作”是指共同致力于实现共同目标的过程。

“协调”和“与...协调”是指共同的决策过程，在此过程中，指定的协调部门或机构负责与受影响的部门和机构合作，以达成共识和一致的行动。

“关键基础设施”在《2001 年爱国者法案》(42 USC 5195c (e)) 中指的是对美国至关重要的物理或虚拟的系统和资产，这些系统和资产的无法运作或破坏将会对安全、国家经济安全、国家公共健康或安全等造成不利影响。

“联邦部门和机构”是指 44 U.S.C. 3502(1)所定义的任何美国机构，而不是 44 U.S.C. 3502(5)所规定的独立监管机构。

“国家基本职能”是指政府职能的一部分，在灾难性的紧急事件中，这些职能对于指导和维持国家安全是必要的。

“主要任务基本职能”是指在紧急事件前、中、后为了支持或实施国家基本职能而履行的政府职能。

“国家安全系统”是指 2002 年《联邦信息安全管理法案》(44 U.S.C. 3542 (b)) 所规定的涵义。

“恢复能力”是指应对和适应不断变化的环境、承受并迅速从破坏中恢复的能力。通信包括承受蓄意攻击、意外、或自然威胁或事故并从中恢复的能力。

“特定行业机构”(SSA)是指该指令中指定的联邦部门或机构，这些部门或机构负责在一切危害环境中提供机构知识和专业知识，以及指导、促进或支持关键基础设施安全和恢复能力计划及相关活动。

“安全的”和“安全”是指用物理方法或网络防御措施应对入侵、攻击、自然或人为灾害，从而降低关键基础设施的风险。

#