路线图

增强抵御僵尸网络的能力

十一月29，2018

目录

I. 背景资料

2017年5月11日，总统发布了第13800号行政命令，“加强联邦网络和关键基础设施的网络安全”，呼吁“抵御僵尸网络和其他自动化，分布式威胁。”总统指示商业和国土安全部部长“领导一个公开透明的过程，识别和促进适当的利益相关者采取行动”，目标是“大幅减少自动化和分布式攻击（僵尸网络）造成的威胁”。[1][2]

商务部和国土安全部共同努力，于2018年5月发布了《关于增强互联网和通信生态系统抵御僵尸网络和其他自动化分布式威胁的抵御力的报告》，即僵尸网络报告。工业和政府，报告呼吁联邦政府明确划定行动重点。这份初始路线图列出了可大幅减少僵尸网络威胁和类似攻击的行动，符合国家网络战略规定的管理优先级。路线图确定了五项工作，每项工作都有一组任务和完成时间表。在此初始版本中，列出了85个任务，但随着一些任务的完成和新任务的产生，该数字会随着时间变化。[3][4]

正如僵尸网络报告所述，该报告的许多行动在设计上相互支持，甚至跨目标。一些行动已经在进行中，其他行动取决于外部因素，最后的决定有待领导和/或资金支持。由于资源限制或相关利益相关方社区的复杂程度不同，我们预计并非所有行动都会同时发生。值得注意的是，尽管这些行动在僵尸网络报告中已经确定，但实施这些行动将使整个互联网生态系统更加安全，其影响将远远超出报告本身的范围。

接下来的路线图列出了与五项努力相关的每项行动的任务：

1. 物联网；
2. 企业；
3. 互联网基础设施；
4. 技术开发和过渡；和
5. 意识和教育。

有些任务将由联邦政府直接负责，而另一些则专门针对私营部门。有些任务并不直接涉及联邦政府，但支持或支持依赖联邦参与或领导的行动。通过表明自己的优先事项，联邦政府可以增强利益相关者的信心，即投入资金用于由联邦政府主导的行业主导行动将产生丰硕成果。

---

1 执行订单号13800，美联储82。注册22,391，截至22,394（2017年5月11日），可用 https://www.federalregister.gov/d/2017-10004.

2 ID。

3 美国商务部和美国国土安全部，致总统的报告，《增强互联网和通信生态系统对僵尸网络和其他自动分布式威胁的抵御能力》（2018年5月），网址：https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets.

4 Nat’l Sec。理事会，《美国国家网络战略》（2018年9月），网址：https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

商务部和国土安全部继续欢迎希望为僵尸网络报告采取行动的私营部门成员的关注。许多路线图行动应由行业，学术界或民间社会牵头。在适用的情况下，本路线图确定了相关任务的现有私营部门领导人或治理结构。如果现有机构已经在采取相关行动，或者已经代表关键社区，则鼓励他们领导。政府有权召集和这样做，但要实现僵尸网络报告规定的结果，需要整个生态系统中的行业和公民社会参与。所识别的任务和相关信息应被视为非约束性和灵活的，以适应数字生态系统随时间的变化。

如果尚未确定由私营部门共同商定的一个或多个政党领导，则联邦政府将提供协调和沟通机制。联邦政府还将定期与有关各方举行会议，促进合作并分享调查结果。在下面的任务突破中被确定为“贡献者”的那些组织不完整地列出为解决方案做出贡献的当前努力。鼓励组织寻找在可行范围内合作的机会。美国政府重视创新，并期望市场为已确定的问题确定最快捷的解决方案。

除了联邦依赖性外，某些行动还具有自然的时间顺序。例如，行动5.1和5.2中的评估计划取决于行动1.1中适当的安全能力基准的建立，因此不能立即开始。其他优先事项的优先工作已经成熟，因为这项工作已经在进行中，例如行动2.2中描述的美国国家标准技术研究院（NIST）网络安全框架（CSF）概况。最后，由于准备周期长（例如，行动1.3、5.3和5.4）或事态发展正在缩小美国影响方向的窗口，因此某些行动具有特别紧迫性（行动1.2）。

最后，为跟踪进展，商务部和国土安全部将为总统制定365天的状态更新，路线图发布后一年。此更新将审查：1）整个社区根据路线图取得的进展；2）这些路线图活动的影响；3）重新评估自动分布式攻击的威胁，包括威胁是在增加还是在减少，以及任何已知的此类改变原因；4）来年应优先开展哪些活动。

II. 路线图

以下小节介绍了从僵尸网络报告中列出的24项行动中采取的五项努力中得出的任务：

1. 物联网；
2. 企业；
3. 互联网基础设施；
4. 技术开发和过渡；和
5. 意识和教育。

这五项工作本身可以细分为由任务组成的工作流。如果任务具有依赖性，则将任务进一步组织为一系列。每个任务描述都包含一个

简短摘要和对僵尸网络报告动作编号的引用，确定任务负责人（如果确定）和支持人员，确定必须开始或完成的任务，并按日历年季度提议开始和完成日期。商务部和国土安全部欢迎利益攸关方就路线图任务的所有方面提供反馈，特别是确定牵头行列和为确定的行动做出贡献的合作伙伴，以及时间表。

物联网工作流：提高物联网安全性标准

僵尸网络报告认识到互联设备对扩展针对生态系统目标的自动分布式攻击范围和规模的影响。物联网（物联网的工作重点是通过建立适用于连接设备整个生命周期的基准安全标准，降低整个物联网生态系统的安全风险。

物联网工作流1：为可信赖的物联网设备开发稳健的市场

该工作流程侧重于为三个领域提供适当安全功能的设备的强劲市场开发：消费者/家庭用户，工业用户和联邦政府。基本初始任务描述了一组核心安全能力，广泛适用（理想情况下，适用于所有三个部门），并可由广泛的评估方案支持。定义核心后，将为三个部门中的每个部门启动并发系列任务。每一系列任务都定义了适用于该领域的核心基准的超集，其后是一系列旨在开发稳健产品一致性市场的支持活动。

定义核心安全能力基准

此任务将建立安全部署物联网设备所需的核心安全功能集，而不管预期的环境如何。通用开发平台应提供或促进核心安全功能，以限制对上市时间的影响并实现创新。这些基准能力还必须适用于基于证明和第三方评估的合格评定方案。

> *任务名称：定义核心安全能力基线*
> 行动编号：1.1
> 任务摘要：比较/分析不同的基线文档，确定可以被全方位评估方案支持的广泛接受的和广泛适用的“核心安全能力”。至少，能力基准可以解决设备和数据安全问题。 NIST将以NIST白皮书或机构间报告（NISTIR）形式发布共识基准，以供将来任务参考和使用。
> 贡献者：NIST（负责人），基准所有者，开发人员套件供应商，消费者财团，数字经济安全理事会（CSDE）/消费者技术协会（CTA）前提任务：无[5]
> 预计开始时间：19年第一季
> 度预期完成时间：19年第三季度[6]

[5]参见安全挖掘委员会。经济，见https://securingdigitaleconomy.org/

[6]所有开始日期均为日历年估计，并取决于资源确定。

僵尸网络路线图

为可信赖的消费者/家庭物联网设备建立稳健的市场

以下任务旨在为具有高产品可用性和强大客户识别度的消费者/家庭物联网产品建立广泛采用的安全

能力基准。这些任务首先通过针对消费者/家庭物联网市场的特定要求增强核心安全能力基线。为鼓励开发和部署兼容设备，将创建认证或评估方案以及教育和意识工具，帮助客户做出明智的物联网购买选择。

任务名称：开发消费者/家庭物联网安全基线
行动编号：1.1
任务摘要：以核心能力为基础，确定适用于消费者/家庭物联网的安全基准。
贡献者：物联网行业，公民社会，NIST，CSDE / CTA前提任务：
发布核心安全能力基线预期开始时间：2016年第二季度
预期竣工时间：2020年第一季度

任务名称：为消费者/家庭物联网设备建立或支持评估计划
动作编号：5.1
任务摘要：为满足上述基准的消费者/家用物联网设备建立或支持敏捷评估或证明计划。
贡献者：行业，公民社会，CTIA，NIST，其他美国政府（USG）利益相关者，CSDE / CTA
前提任务：制定消费者/家庭物联网安全基线预期开始：进行中
预期竣工时间：2020年第二季度

任务名称：探索消费者/家庭物联网标签
动作编号：5.1
任务摘要：探索自愿性标签方法或其他信息选项的效用，以提高消费者/家庭物联网设备消费者的意识。
贡献者：联邦贸易委员会（FTC），NTIA，其他联邦合作伙伴，物联网行业，零售商，民间社会，学术界，CSDE / CTA
必备任务：N / A
预计开始时间：19年第三季度
预期完成时间：20年第二季度

任务名称：为可信赖的消费者/家庭物联网设备实施意识战略
动作编号：5.1
任务摘要：开发信息工具，如标签或品牌，以帮助有动机的消费者识别符合标准的消费者/家庭物联网产品。
投稿人：物联网行业，零售商，CSDE / CTA
前提任务：建立消费者/家庭物联网设备评估计划；探索消费者/家庭物联网的标签
预计开始时间：20年第二季
度预期完成时间：21年第二季度

任务名称：联邦消费者/家庭物联网安全基线和评估支持

操作编号：5.5
任务摘要：加强美国政府与目标用户社区和民间社会的互动，促进消费者/家庭物联网安全基线和支持评估计划的认识和接受；利用DHS现有的认知活动，如STOP.THINK.CONNECT。 贡献者：国土安全部，商业，FTC，民间社会
前提任务：制定消费者/家庭物联网安全基线；建立家庭物联网设备评估计划。
预计开始时间：20年第二季
度预期完成时间：23年第一季度

为可信赖的工业物联网设备建立稳健的市场

以下任务旨在为具有高产品可用性和强大客户认可度的工业物联网产品建立广泛采用的安全能力基准。这些任务首先通过针对工业物联网市场的特定要求扩展核心安全能力基线。为鼓励开发和部署兼容设备，创建了一个或多个评估方案以及教育和意识工具，以告知客户。

任务名称：开发工业物联网安全基准
行动编号：1.1
任务摘要：以核心能力为基础，确定适用于工业/ SCADA环境的安全基准。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：发布核心安全能力基线预计开始时间：2016年第二
季度
预期完成时间：19年第四季度

任务名称：建立工业物联网设备评估计划
行动编号：5.2
任务摘要：为满足基线要求的工业物联网设备建立具有成本效益的评估计划。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：制定工业物联网安全基线预计开始时间：19年第四
季度
预期竣工时间：20年第二季度

任务名称：探索工业物联网设备的标签或其他透明度方案
行动编号：5.2
任务摘要：努力开发一种自愿标签方法或其他信息透明模式，作为通知工业企业客户的一种选择。
贡献者：工业物联网行业，国家实验室，国土安全部，行业特定机构，行业协调委员会（例如，能源，健康，运输）
前提任务：制定工业物联网安全基线预计开始时间：19年第四
季度
预期竣工时间：20年第二季度

任务名称：工业物联网设备客户支持意识
行动编号：5.2
任务摘要：创建信息工具（如标签或品牌），帮助工业企业客户识别合格的工业物联网产品。
贡献者：工业物联网行业，零售商，国家信息共享和分析中心理事会（ISACs）的国土安全部
前提任务：制定工业物联网安全基线
预计开始时间：20年第二季度
预期竣工时间：20年第二季度

任务名称：促进关键基础设施采用评估制度
行动编号：5.2
任务摘要：通过物联网和信息技术产品（ISAT）理事会，国土安全部和工业界将评估物联网和信息技术产品在关键基础设施上的适用性时的商业认证制度。
贡献者：国土安全部（领导层），工业物联网行业，国家实验室，国土安全部，行业特定机构，部门协调委员会（例如，能源，健康，运输）
前提任务：建立工业物联网设备评估计划
预计开始时间：20年第三季度
预期竣工时间：23年第一季度

为可信赖的联邦物联网设备建立稳健的市场

下列任务旨在为具有高产品可用性和强大客户认可度的联邦物联网产品建立广泛采用的安全能力基准。这些任务首先通过针对联邦物联网市场的特定要求增强核心安全能力基线。为鼓励采购和部署合格设备，建立了以联邦基准为基础的联邦采购法规。

任务名称：识别联邦物联网安全要求
操作编号：2.3
任务摘要：在一系列会议中召集关键利益相关者，确定联邦环境通用/特定的非核心安全功能。
贡献者：管理和预算办公室（OMB），总务管理局（GSA），国防部（DOD），国土安全部，国家标准与技术研究院（NIST），联邦首席信息官（CIO）理事会，联邦首席信息安全官（CISO）
前提任务：发布核心安全能力基线
预期开始：待定
预期竣工时间：待定

任务名称：指定联邦物联网安全能力基准
操作编号：2.3
任务摘要：与行业和机构合作，制定和发布联邦物联网安全能力基线。
贡献者：NIST（负责人），国土安全部，联邦CIO理事会，联邦CISO，行业，CSDE / CTA前提任务：确定联邦物联网安全要求
预计开始时间：19年第三季度预期完成时间：20年第一季度

任务名称：建立联邦物联网采购法规
操作编号：2.3
任务摘要：建立联邦采购法规，支持符合联邦物联网安全能力基准的物联网设备采购。
投稿人：GSA（领导），OMB，联邦CIO委员会，联邦CISO和采购人员前提任务：指定联邦物联网安全能力基准
预计开始时间：待定预计完
成时间：待定

物联网工作流2：物联网安全的采用和可持续性

此工作流程总体上侧重于物联网设备全球生态系统的开发。也就是说，此工作流程中指定的一系列操

作可增强物联网产品的安全性，并增强对物联网市场的信心，而无需考虑三个特定于部门的安全基准。任务重点是网络安全和运营技术社区之间的协作，以及国际政策倡导，统一和标准。除了制定全球相关的物联网标准外，这些活动几乎没有依赖性。一个关键挑战将是确定活动的优先级以反映资源可用性。

扩展物联网风险管理

许多企业网络安全计划已转向基于风险的方法，例如NIST的网络安全框架。这些组织利用框架和相关方法来管理与网络安全相关的风险的标准，准则和最佳实践，历来集中于信息技术和传统信息网络。在这一系列任务中，扩展了风险管理方法，以帮助组织更好地理解和管理与物联网设备整个生命周期相关的网络安全和隐私风险。

任务名称：为物联网安全启用风险管理方法
动作编号：1.5
任务摘要：发布NISTIR 8228，“管理物联网（物联网网络安全和隐私风险的考虑因素”，以支持物联网安全的风险管理方法。贡献者：NIST（行业），行业
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第一季度

任务名称：为物联网设备制造商发布最佳实践
动作编号：1.5
任务摘要：使用核心安全功能，识别有助于新兴NISTIR 8228“管理物联网（物联网网络安全和隐私风险的考虑因素”中确定的客户成果的最佳实践。
投稿人：NIST（负责人），待定
前提任务：为物联网安全启用风险管理方法；发布核心安全能力基准
预计开始时间：19年第二季
度预期完成时间：20年第二季度

任务名称：商品化安全更新技术

动作编号：1.5
任务摘要：促进安全更新的标准和商业框架。鼓励物联网开发人员套件采用安全更新机制，以最大程度地缩短开发人员的上市时间。为物联网设备安全更新发布互联网工程任务组（IETF）规范，鼓励对安全补丁进行现成支持。
贡献者：IETF参与者，NIST，NTIA，其他先决任务：不适用
预计开始时间：正在进行中
预期完成时间：2016年第二季度

任务名称：使可用性和可管理性与客户能力保持一致
操作编号：3.2
任务摘要：为面向家庭和小型企业的设备提供简单，直接的部署和配置流程优先级。
贡献者：消费者技术协会（CTA），IT和物联网行业
前提任务：N / A
预期开始：进行中
预期完成：持 续

建立全球相关的物联网标准

僵尸网络报告指出，“政府和行业应与行业主导的自愿性国际标准和规范开发商共同参与，建立全球相关标准。”这一系列任务鼓励美国政府和行业共同遵循与上一工作流程中制定的能力基准相一致的国际标准。

任务名称：建立全球相关的物联网标准
操作编号：1.2
任务摘要：美国政府和业界应通过包容性讨论过程，共同确定一组自愿制定国际物联网安全标准的关键场所，并发起标准活动。基线完成后，参与者可以引入核心安全能力基线作为贡献。
投稿人：NIST，NTIA，DHS，IICSWG，物联网行业
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第四季度
任务名称：识别鼓励物联网采用安全标准的措施
操作编号：2.3
任务摘要：确定私有部门采用物联网安全标准和基线的现有和必要激励措施，USG可以采用。 贡献者：物联网行业，国土安全部，商务，FTC，行业特定机构，行业协调委员会
前提任务：建立全球相关的物联网标准
预计开始时间：待定
预期竣工时间：待定

企业努力路线

企业努力路线专注于可以在企业管理级别采取的行动，以减少僵尸网络和自动化，分布式攻击对企业和生态系统的总体风险。

企业努力路线有四个互补的工作流程：

- 用于缓解和保护的CSF配置文件
- 迁移到高级企业网络架构
- 联邦采用企业最佳实践
- 运营技术

企业工作流1：用于缓解和保护的CSF配置文件

NIST网络安全框架已成为企业和机构采用基于风险的方法来实现适当的安全成果的重要工具。这一系列任务建立行业共识的CSF配置文件，以缓解分布式拒绝服务（DDoS）威胁和对抗僵尸网络。在完成行业主导的档案后，联邦政府针对联邦环境量身定制这些档案。

任务名称：为分布式拒绝服务缓解开发CSF配置文件
操作编号：2.2
任务摘要：与业界合作，开发用于分布式拒绝服务缓解的共识性CSF配置文件。贡献者：网络安全联盟（领导），数字生态系统行业，NIST，NTIA，DHS，民间社会[7]
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第一季度

任务名称：为分布式拒绝服务缓解发布联邦CSF配置文件
操作编号：2.3
任务摘要：作为NIST特殊出版物发布用于分布式拒绝服务缓解的联邦CSF配置文件。贡献者：NIST（负责人），国土安全部，联邦机构，数字生态系统利益相关者，公民社会前提任务：为分布式拒绝服务缓解开发CSF配置文件
预计开始时间：2016年第二季度
预计完成时间：19年第三季度

任务名称：为僵尸网络威胁缓解开发CSF配置文件
操作编号：2.2
任务摘要：为僵尸网络威胁缓解开发行业共识的CSF配置文件。贡献者：网络安全联盟（领导），数字生态系统利益相关者，NIST，NTIA，DHS，民间社会
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第二季度

[7]参见网络安全联盟，网址：https://www.cybersecuritycoalition.org/

任务名称：发布僵尸网络威胁缓解联邦CSF配置文件
操作编号：2.3
任务摘要：作为NIST特殊出版物发布联邦僵尸网络用于缓解僵尸网络威胁。
贡献者：NIST（负责人），国土安全部，联邦机构，数字生态系统利益相关者，民间社会
前提任务：为缓解僵尸网络威胁制定CSF配置文件
预计开始时间：2016年第二
季度预计完成时间：19年第三季度

任务名称：提高企业对分布式拒绝服务缓解的意识
操作编号：3.3
任务摘要：建立合作伙伴关系活动和战略参与活动，以提高用户和企业对自动化分布式威胁和最佳安全实践的了解。
贡献者：网络安全联盟，NTIA，DHS，NIST，民间社会
前提任务：N / A
预期开始：进行中
预期完成时间：待定

企业工作流2：推进企业网络架构

企业应迁移到有助于检测，破坏和缓解自动化分布式威胁的网络体系结构。他们还应该考虑自己的网络如何使他人面临风险。在此工作流中，一系列并行活动确定当前最佳实践并探索企业网络架构的新兴技术。

任务名称：增强和发展企业网络流量管理最佳实践
动作编号：3.1
任务摘要：牢记小型企业的需求，针对目标生态系统部门，增强和发展有关企业网络流量管理的建设性政策和最佳实践。随着技术和架构的发展，不断发展最佳实践，并为新参与者和新进入者填补最佳实践中的空白。
贡献者：CSDE / CTA（领导），行业协调小组，企业网络运营商，网络运营商团体（NOG），网络工程师，NIST，NTIA，DHS，DOD，互联网服务提供商，基础设施提供商，全球数字生态系统企业，民间社会
前提任务：不适用
预计开始时间：正在进行中
预期完成时间：2019年第二季度

任务名称：促进减轻自动化，分布式威胁风险的企业网络架构
操作编号：3.3
任务摘要：促进高级企业网络架构的实施和采用，以减轻自动化，分布式威胁的风险。确定企业采用差距激增的地方，并努力了解整合和部署的市场和政策障碍。
贡献者：CSDE，行业协调机构，企业网络工程师和运营商，NOG，NTIA，NIST，DHS，国家安全系统委员会（CNSS），学术界，民间社会

前提任务：增强和发展网络流量管理最佳实践
预计开始时间：2019年第二季度
预期竣工时间：待定

任务名称：加速IPv6互联网服务在国内的可用性
操作编号：3.4
任务摘要：政府与利益相关方合作，通过识别从行业和其他国家汲取的经验教训，确定过渡障碍和潜在激励措施，支持互联网服务提供商向IPv6全面过渡。
投稿人：NTIA（领导），区域互联网注册管理机构（RIR），互联网服务提供商，信息技术和物联网行业
前提任务：N / A
预计开始时间：19年第四季
度预计完成时间：20年第二季度

任务名称：加速过渡到IPv6企业网络
操作编号：3.4
任务摘要：演示纯IPv6企业IT部署的影响和实用性。贡献者：NIST（行业），行业
前提任务：N / A
预期开始：待定预期
完成时间：待定

任务名称：建立零信任网络要求（ZTN）
操作编号：3.3
任务摘要：联邦CIO理事会零信任网络工作组将制定代理部署零信任网络（ZTN）的初始要求。使用这些要求，部门和机构将可以在响应技术出现时整合这些功能。
贡献者：联邦CIO理事会零信任网络工作组（负责人）[8]
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：2018年第四季度

任务名称：评估ZTN的当前可行性
操作编号：3.3
任务摘要：美国国家网络安全卓越中心（NCCoE）和行业合作者将针对CTN理事会ZTN工作组使用商业和新兴技术确定的ZTN要求进行可行性研究。
贡献者：NIST（负责人），国土安全部（DHS），首席信息官（CIO）理事会零信任网络工作组
前提任务：建立零信任网络的要求
预计开始时间：正在进行中
预期完成时间：19年第四季度
任务名称：确定物联网网络管理最佳实践 动作编号：1.5

[8] 参见CIO理事会关于理事会，网址：https://www.cio.gov/about/.

任务摘要：NIST将使用NCCoE缓解基于物联网的分布式拒绝服务项目结果和ZTN可行性研究，为环境包括物联网设备的企业网络管理确定当前最佳实践。
贡献者：NIST（负责人），国土安全部，数字生态系统行业和民间社会利益相关者。
缓解基于物联网的分布式拒绝服务（DDoS）
预计开始时间：3Q19
预期竣工时间：20Q2

企业工作流3：联邦采用企业最佳实践

利益相关者表示，联邦采用“好邻居”做法将为整个生态系统基础架构，为开展进一步活动减少自动化，分布式威胁提供基础。尤其是，联邦机构实施出口过滤以防止网络地址欺骗，关闭用于放大流量的反射器并衡量机构合规性（以及可能有名无实的不良行为者）的措施，将表明联邦政府决心并鼓励其他各方采取有益行动。在这一系列任务中，联邦政府开展活动，确保这些最佳实践在联邦机构的政策，标准，指南和监督中得到适当体现。

任务名称：联邦针对自动化分布式威胁采用联邦CSF配置文件
操作编号：2.3
任务摘要：OMB向机构发布有关采用联邦CSF配置文件自动分发威胁的指南，包括采用和报告时间表。 NIST创建或识别用于量化进度的度量工具。
贡献者：OMB e-Gov（领导），NIST，DHS和其他USG机构
前提任务：分布式拒绝服务缓解联邦CSF配置文件；联邦CSF僵尸网络预防和缓解简介
预期开始：进行中
预期完成时间：20年第二季度
任务名称：在所有美国联邦代理网络中实施入口/出口过滤
操作编号：2.3
任务摘要：联邦机构确保代理机构网络和商业配置的网络信息服务采取积极措施，防止网络源地址带有欺骗性流量。
贡献者：DHS（领导），GSA，OMB，其他联邦机构，联邦合同服务提供商
前提任务：N / A预计
开始时间：正在进行中
预期完成时间：19年第三季度

任务名称：制定反射器联邦安全指南
操作编号：2.3
任务摘要：通过NIST特殊出版物补充现有的NIST指南，用于操作域名系统（DNS）服务器和解析器，为网络时间协议（NTP）和其他广泛部署的用户数据报协议（UDP）资源的运行制定通用指南。
贡献者：NIST（负责人），国土安全部（DHS）
前提任务：N / A
预期开始：进行中

预期竣工时间：19年第二季度

任务名称：实施反射器联邦安全指南
操作编号：2.3
任务摘要：授权所有联邦机构执行NIST反射资源指南。
贡献者：国土安全部（共同领导），OMB（共同领导），NIST
前提任务：为反射器制定联邦安全准则预计
启动时间：19年第二季度
预期竣工时间：20Q2
任务名称：跟踪和补救联邦机构的脆弱资源
操作编号：2.3
任务摘要：使用不符合NIST指南的反射资源编制联邦机构清单，并跟踪进度。 贡献者：国土安全部（牵头），OMB，美国各部门和机构
前提任务：针对自动化分布式威胁采用联邦CSF配置文件
预计开始时间：20年第二季度
预期完成：正在进行中

企业工作流4：运营技术

下面指定了一系列任务，以缩小网络安全与运营技术（OT）社区之间的理解差距。网络安全专家通常对OT特定问题（例如安全）所施加的限制和约束知之甚少，而运营技术界对网络安全风险和能力的认识有限。

任务名称：网络安全与OT社区合作，增进对OT网络安全挑战的理解
操作编号：4.5
任务摘要：网络安全社区与OT社区合作，增进对网络安全挑战的理解。
贡献者：国土安全部（领导），部门特定机构，国家实验室，部门协调理事会
前提任务：无
预计开始时间：19年第二季
度预期完成时间：21年第三季度
任务名称：扩展OT-网络安全信息共享
操作编号：4.5
任务摘要：扩大当前联邦政府的活动，以促进旧约和网络安全社区之间的信息共享。
贡献者：国土安全部（领导），部门特定机构，国家实验室，部门协调理事会
前提任务：无
预计开始时间：19年第二季
度预期完成时间：21年第三季度
任务名称：促进信息技术安全技术的旧约采用
操作编号：4.5

任务摘要：扩大当前促进旧约采用IT安全技术的联邦参与。
贡献者：NIST（负责人），国土安全部，行业特定机构，行业协调委员会
前提任务：无
预期开始：进行中
预期完成时间：21年第三季度

基础设施工作线

基础设施工作线专注于需要在广泛的数字生态系统参与者之间进行协调或影响全球数字基础设施核心功能的行动。

基础设施工作线有四个互补的工作流程：

- 改进路由安全性
- 实践中的信息共享
- 信息共享协议
- 研究与开发

基础设施工作流1：改进路由安全性

互联网旨在促进端点之间的弹性通信，并较少关注基本安全服务。结果，互联网上路由安全的状态远远低于使用常见和较新的工具和实践所能达到的水平。这一系列任务将促进长期部署反欺骗技术和较新技术的部署，以防止路由劫持和泄漏。

任务名称：消除采用资源公钥基础设施（RPKI）的法律和政策障碍
操作编号：2.3
任务摘要：建立共识法律策略以解决采用RPKI的障碍，包括为遗留地址持有者颁发RPKI证书，负债问题以及替代部署模型的障碍。
投稿人：学术界，互联网工程师，NIST，NTIA，DOD，区域和本地互联网登记
先决条件任务：N / A
预计开始时间：19年第二季度
预期完成时间：20年第二季度

任务名称：联邦机构采用RPKI
操作编号：2.3
任务摘要：联邦地址持有者和服务提供商为地址资源创建路由来源授权（ROA），并将ROA应用于互联网路由决策，以缓解路由劫持。
贡献者：国土安全部（领导），OMB，国防部，联邦机构
前提任务：消除采用RPKI的法律和政策障碍预计
开始时间：20年第一季度
预期竣工时间：21年第一季度

任务名称：提高反欺骗机制的可扩展性和稳健性
操作编号：2.3
任务摘要：政府和行业持续研究以使反欺骗更具可扩展性和健壮性，并在互联网的所有级别可用。
贡献者：国土安全部（领导），联邦技术孵化器，NIST，互联网工程师，学术界
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第四季度

任务名称：扩展反欺骗机制的采用，意识和应用
操作编号：2.3
任务摘要：酌情在整个互联网基础设施中推广采用和扩展反欺骗机制的实施。
投稿人：互联网基础设施所有者和运营商，民间社会，NIST，NTIA，DHS
前提任务：提高反欺骗机制的可扩展性和健壮性
预计开始时间：19年第四季度
预期竣工时间：20年第二季度

*任务名称：建立相互同意的路由安全规范（MANRS）天文台和仪表板，制定路由安全指标*动作编号：2.5
任务摘要：开发指标和网站，以评估互联网路由系统随时间推移的安全性和弹性。
贡献者：互联网协会，RIR
前提任务：N / A
预期开始：进行中
预期完成时间：2018年第四季度

任务名称：制定互联网服务安全要求
操作编号：3.3
任务摘要：发布SP 800-189，“安全的域间流量交换：BGP稳健性和分布式拒绝服务缓解”。 贡献者：NIST（领导）
前提任务：N / A
预期开始：进行中
预期完成时间：19年第二季度

任务名称：探索围绕路由安全的威胁演变和新兴解决方案
操作编号：3.3
任务摘要：与利益相关者和互联网基础设施参与者互动，了解现有和新兴路由安全解决方案的优势和局限，捕捉利益相关者的担忧和潜在缓解措施。
贡献者：NTIA，互联网基础设施所有者和运营商，公民社会，NIST，DHS
前提任务：N / A
预计开始时间：19年第三季度
预期完成时间：20年第三季度

基础设施工作流2：实践中的信息共享

大型网络提供商目前共享对特定威胁有效的网络管理技术和防御策略。执法依靠私营部门的信息发起调查。这一系列任务的重点是将信息共享扩展到较小的ISP和外部网络提供商，并确保在尽早通知执法部门，同时尊重隐私准则和法规。

任务名称：增加小型互联网服务提供商（ISP）访问行业共享威胁信息的机会
行动编号：2.1
任务摘要：扩大国内信息共享，增强小型互联网服务提供商的参与。贡献者：基础设施提供商，通过通信ISAC的DHS
前提任务：N / A
预期开始：待定预期
完成时间：待定

任务名称：扩展全球和区域威胁信息共享
行动编号：2.1
任务摘要：加强信息共享机制，促进扩大的全球和区域共享。
贡献者：全球计算机安全事件响应小组（CSIRT），DHS，NOG，ISAC，基础设施提供商 先决条件任务：N / A
预计开始时间：19年第一季度
预期完成时间：待定

任务名称：展开信息共享协议
行动编号：2.1
任务摘要：美国政府利用ISAC，NOG合作伙伴关系，事件响应和安全团队论坛（FIRST），并与国际同行合作，扩大信息共享协议。
贡献者：DHS，NOG，ISAC委员会，ISAC，FIRST，执法合作伙伴，网络中心/融合中心
前提任务：N / A
预期开始：待定
预期完成时间：待定

任务名称：与执法部门共享及时可行的信息
行动编号：4.1
任务摘要：提供更加及时和可操作的信息，以促进，支持和加速执法行动，包括影响分布在全球的僵尸网络的行动。
投稿人：司法部（DOJ）/联邦调查局（FBI），FTC，ISAC，DHS，NOG，全球CSIRT，大型企业和基础设施提供商
前提任务：N / A
预期开始：待定预期
完成时间：待定

任务名称：改善美国政府与行业的信息共享
行动编号：4.1
任务摘要：提高美国政府与行业共享信息的及时性和相关性。
贡献者：USG网络中心，国土安全部，行业特定机构，ISAC /信息共享和分析组织（ISAO）
前提任务：N / A
预期开始：待定
预期完成时间：待定
任务名称：提高安全关键数据资源的准确性
行动编号：4.1
任务摘要：WHOIS数据库由互联网命名和编号资源（例如，IP地址和域名）的注册信息组成，为提高准确性，促进了不良行为者的归因。建立了机制，在满足隐私保护法规（例如，欧盟通用数据保护法规[GPDR]）并支持僵尸网络调查工作的同时，能及时获取WHOIS信息。
投稿人：域名注册机构/注册商，NTIA，互联网名称与数字地址分配机构（ICANN），RIR，执法，学术界和公民社会
必备任务：N / A
预期开始：正在进行中
预期完成：正在进行

基础设施工作流3：信息共享协议

这些任务集中于信息共享协议的标准化，以提高速度并允许自动响应。增强信息共享协议的效用通过增加共享信息的价值来补充信息共享流程任务。

任务名称：支持信息共享自动化
行动编号：2.1
任务摘要：增强信息共享协议以提高速度并支持自动响应。
贡献者：国土安全部，国际民航组织，工业，民间社会，财团
前提任务：不适用
预计开始时间：待定预计完
成时间：待定

任务名称：支持协作事件响应
行动项目：4.4
任务摘要：IETF最终确定分布式拒绝服务开放威胁信令（DOTS）协议。拥有多方分布式拒绝服务缓解策略的企业将实施和部署DOTS，以促进协调行动。
贡献者：IETF，数字生态系统企业，民间社会
前提任务：无
预期开始：进行中
预期完成时间：待定

任务名称：增强信息共享协议，促进全球信息共享
操作编号：2.4
任务摘要：美国政府和行业将审核和增强信息共享协议，例如结构化威胁信息表达（STIX）和可信的指标信息自动交换（TAXII），以促进有关自动化威胁的全球信息共享。
贡献者：国土安全部（领导），国际民航组织，联邦资助的研发中心（FFRDC），工业
前提任务：N / A预期开始：
待定预期完成时间：待定

任务名称：建立国际标准以促进信息共享
操作编号：2.4
任务摘要：行业将在美国政府的支持下建立信息共享的国际标准，促进全球协调。
贡献者：行业（牵头），国土安全部，ISAC / ISAO，民间社会前
提任务：不适用
预计开始时间：待定预计完
成时间：待定

基础设施工作流4：研发

任务名称：将基础设施最佳实践纳入NIST网络安全框架
操作编号：3.3
任务摘要：持续评估最佳安全实践和技术的进步，纳入NIST网络安全框架。
投稿人：NIST（负责人），基础设施提供商
前提条件任务：N / A
预计开始时间：待定
预计完成时间：待定

任务名称：通过透明度和可追踪性破坏攻击者生态系统
操作编号：4.4
任务摘要：自动化分布式威胁生态系统偏向攻击者。这项任务旨在开发方法，破坏传统上用来发起僵尸网络的生态系统（如游戏社区），并通过透明和责任制为攻击者增加风险。工业界和政府共同在相关的多利益相关方论坛中倡导更广泛地实施破坏攻击者工具和激励措施的措施。
投稿人：ICANN，RIR，NTIA，执法，FTC
前提任务：N / A
预计开始时间：待定
预计完成时间：待定

技术开发和工作转型线

技术开发和转型的努力方向有三个互补的工作流程：

- 建立安全的软件市场
- 国际协调
- 研究与开发

技术开发和过渡工作流1：建立安全软件市场

这一系列任务为通过安全软件开发实践开发的系统和应用程序建立强大而可持续的市场。任务建立安全软件开发公认的准则，提高安全软件开发工具的效率和有效性，以增加投资回报，并在政府赞助的技术论坛中展示这些进步。

任务名称：建立安全软件开发生命周期准则
操作编号：1.3
任务摘要：NIST与行业合作，将安全软件开发生命周期指南定义为NIST特殊出版物。
贡献者：NIST（负责人），国土安全部（DHS），
行业
先决任务：不适用
预期开始：进行中
预期完成时间：20年第二季度

任务名称：开发软件组件透明度准则
操作编号：1.3
任务摘要：探索制造商和供应商如何交流现代软件和物联网设备中第三方软件组件的有用且可操作的信息，以及企业如何使用这些数据来制定更好的安全决策和实践。
贡献者：NTIA（领导），关键基础设施部门，数字生态系统利益相关者
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：2016年第二季度

任务名称：填补软件开发工具中的空白
操作编号：1.3
任务摘要：网络和信息技术研究与开发计划（NITRD）将为软件开发工具促进有针对性的研究资金和协作技术过渡活动，以高效有效地采用安全软件开发生命周期（SSDLC）。
贡献者：NITRD（领导）
前提任务：N / A
预期开始：进行中
预期完成时间：23年第一季度

任务名称：增强软件开发工具链

操作编号：1.3
任务摘要：通过管理软件开发工具链的公开竞争，加速开发和采用有效高效的软件开发技术。
贡献者：NIST（负责人），国土安全部（DHS）
前提任务：N / A
预期开始：进行中
预期完成时间：22年第一季度

任务名称：展示安全编码实践方面的进展并共享有关安全风险的信息
行动编号：5.3
任务摘要：展示由学术界和安全研究人员开发的安全编码实践和工具方面的先进技术，并在年度PrivacyCon会议上共享有关安全风险的信息。
贡献者：FTC（领导）
前提任务：N / A
预计启动时间：19年第三季度
预期完成时间：正在进行

任务名称：机构需要安全开发政府现货（GOTS）软件
操作编号：2.3
任务摘要：针对鼓励或强制性应用SSDLC的GOTS软件开发合同制定了联邦采购法规。贡献者：GSA，OMB，国防部，美国其他部门和机构
前提任务：定义核心安全能力基线
预期开始：待定
预期竣工时间：待定

任务名称：代理商采购安全开发的商业现货（COTS）软件
操作编号：2.3
任务摘要：针对喜欢或需要使用SSDLC开发的COTS软件采购制定联邦采购法规。
贡献者：GSA（领导），OMB，DHS（连续诊断和缓解计划），国防部，美国其他部门和机构
前提任务：定义核心安全能力基线
预期开始：待定
预期竣工时间：待定
任务名称：开发报废软件最佳实践
动作编号：1.5
任务摘要：为平衡客户和业务需求的失效和孤立软件和设备开发一系列寿命终止流程。 投稿人：CTA，NTIA，其他政府和行业参与者
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：19年第四季度

技术开发和过渡工作流2：国际协调

任务名称：改善现有的美国政府在国际标准上的协调
行动编号：4.2
任务摘要：在机构间国际网络安全标准化工作组（IICSWG）的工作基础上，进一步改善美国政府与国际标准机构合作的协调。确定在这些机构中促进行业驱动标准制定的策略。
投稿人：NIST（牵头），IICSWG成员机构
前提任务：N / A
预期开始：进行中
预期完成：持续

任务名称：优化行业-USG标准协调
行动编号：4.2
任务摘要：为参与国际标准制定的美国行业实体和联邦机构建立持续协调的框架和策略。贡献者：NIST，NTIA，州，IICSWG，行业，CSDE，行业协会
必备任务：N / A
预期开始：正在进行中
预期完成：正在进行

任务名称：通过双边和多边国际参与促进国际最佳做法采用
行动编号：4.2
任务摘要：通过双边，多边和多利益相关方的参与，促进采用国际公认的最佳实践，并利用美国政府集团各机构的专业知识。
贡献者：州，NTIA，NIST，行业，公民社会
前提任务：N / A
预期开始：进行中
预期完成时间：待定

任务名称：在全球范围内促进对特定既有工具，协议和最佳实践的认识和采用
操作编号：3.3
任务摘要：促进大规模解决自动化网络风险的既有工具，协议和最佳实践的实施和采用。制定易于理解的实施指南，并与世界各地的利益相关方合作。发展衡量此实施影响的能力。 贡献者：全球网络联盟，行业协调机构，NTIA，NIST，DHS
先决任务：N / A
预期开始：进行中
预期完成：持续

任务名称：在国际上推广域名系统最佳实践
行动编号：4.2
任务摘要：通过美国在ICANN，IETF和互联网治理论坛等多方利益相关方论坛上推广域名系统的最佳实践和相关工具。

贡献者：NTIA（领导），政府和私营部门多方利益相关者参与者
前提任务：不适用
预期开始：进行中
预期完成：持续

技术开发和过渡工作流3：研发

基于物联网的僵尸网络提供的分布式拒绝服务容量的快速增长削弱了当前分布式拒绝服务缓解技术的有效性。为了领先于恶意行为者，迫切需要进行缓解技术的研发，或者利用新数据分析，机器学习或人工智能。需要行业主导的研究活动才能开发和部署创新技术。作为网络安全基础研究的重要资金来源，联邦政府应通过有针对性的资助和协作式技术转换活动来支持这一行动。

任务名称：加速缓解分布式威胁的联邦资助研发
行动编号：1.4
任务摘要：针对缓解自动化分布式威胁的技术，促进有针对性的研究资金和协作技术过渡活动。
贡献者：NITRD（负责人），美国国土安全部，美国各部门和机构
前提条件任务：N / A
预期开始：进行中
预期完成：持续

任务名称：加速开发和部署预防和缓解分布式威胁的创新技术
行动编号：1.4
任务摘要：工业界，学术界和政府应加快开发和部署创新技术，预防和缓解分布式威胁。贡献者：竞争环境中的生态系统参与者
必备任务：N / A
预期开始：正在进行中
预期完成：正在进行

任务名称：增加流量管理责任制
动作编号：2.5
任务摘要：检查自治系统，互联网对等互连和传输协议在多大程度上可以改善流量管理责任制。
投稿人：NOG，联邦技术孵化器，国土安全部，公民社会，学术界
前提任务：N / A
预计开始时间：待定
预计完成时间：待定

任务名称：加速行业研发以缓解分布式威胁
行动编号：1.4
任务摘要：加快开发和部署创新技术，预防和缓解分布式威胁。
投稿人：行业协会和实验室，学术界

前提任务：N / A
预期开始：待定预期
完成时间：待定

任务名称：优先考虑技术转换
动作编号：2.5
任务摘要：强调技术过渡策略是网络流量管理新工具和新实践研究计划的关键组成部分。
投稿人：工业，政府和民间社会联盟待定
前提任务：N / A
预计开始时间：待定
预计完成时间：待定
任务名称：促进新兴最佳实践
行动编号：1.4
任务摘要：随着技术成熟和最佳实践的出现，加大研究和技术转换的力度。
贡献者：民间社会待定前提任务：N / A
预期开始：进行中
预期完成：正在进行

意识和教育努力

意识和教育努力范围有两个互补的工作流程：

- 提升消费者信心
- 教育劳动力

意识和教育工作流1：提升消费者信心

消费者对物联网设备安全性缺乏信心可能会阻碍物联网的采用。这一系列任务的重点是建立消费者信心，使消费者能够识别满足需求的产品，遵守供应商的安全声明，并通过应用商业可用的网络安全技术提供真正的保护。

任务名称：促进适当的产品部署
操作编号：4.3
任务摘要：对消费者进行不同的基线和评估计划教育，以表明所部署的产品正在使用适当的安全性。
贡献者：特定领域的机构，民间社会，消费者团体，FTC，DHS，NTIA，CTA。建立工业物联网设备评估计划；指定物联网安全能力基准
预计开始时间：20年1季度预
计完成时间：23季度

任务名称：制止非法营销行为
操作编号：4.3

任务摘要：通过执法行动制止和阻止物联网和信息技术供应商的非法营销行为。
贡献者：FTC（领导）
前提任务：N / A
预期开始：进行中
预期完成：正在进行

任务名称：缓解基于物联网的分布式拒绝服务
动作编号：1.5
任务摘要：演示结合制造商使用说明（MUD），威胁信号，安全更新和基本网络卫生的影响和实用性，以保护物联网设备并减轻受损的物联网设备的影响。
贡献者：NIST（领导），公民社会，互联网工程师
前提任务：N / A
预期开始：进行中
预期完成：持续

意识和教育工作流2：教育劳动力

随着各种各样的产品和服务上线，新型产品中会出现网络安全威胁。产品设计师沉迷于与产品相关的传统风险，但通常不知道当产品连接到网络时可能引入的新风险。这一系列任务的重点是对现有和新兴劳动力（无论工程学科如何）进行基本网络安全教育。

任务名称：准备编程人员
操作编号：1.3
任务摘要：在整个学习过程中的编程课程中纳入设计安全原则和支持工具。 贡献者：学术界，安全软件开发社区，培训和认证提供商，认证机构，政府
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：20年第二季度

任务名称：准备工程人员
行动编号：5.4
任务摘要：在所有工程学科的学习过程中纳入网络安全原则。
投稿人：学术界，联邦和州政府
前提任务：N / A
预期开始：进行中
预期完成时间：20年第二季度
任务名称：根据员工需求调整课程
行动编号：5.3

任务摘要：继续促进国家网络安全教育倡议（NICE）框架，作为开发课程内容（尤其是软件开发方面）的参考工具。
贡献者：NIST（领导），学术界，认证机构，专业协会，认证提供者
前提任务：N / A
预计开始时间：正在进行中
预期完成时间：2018年第四季度

任务名称：建立工程师网络安全教育计划
行动编号：5.4
任务摘要：将网络安全作为所有工程学科的基本要求，并为工程师创建或利用现有的在线网络安全培训。
投稿人：NIST，网络安全教育界，认证计划
前提任务：N / A
预期开始：进行中预期完成
时间：21年第一季度

III. 后续步骤

商务部和国土安全部将与其他美国政府机构和私营部门合作，协调和跟踪路线图活动。国土安全部将跨部门特定机构与关键基础设施组织进行协调。商务部将通过NIST协调标准和技术活动，并将通过NTIA跨政府和数字经济进行协调。

我们还将定期提供更新，包括：

- 定期与私营部门利益相关者举行会议和沟通，私营利益相关者领导着共享信息和进步的关键举措。
- 在中期（路线图发布后大约六个月）召集利益相关者，通过研讨会或其他会议讨论路线图实施进展。
- 根据僵尸网络报告的详细情况，在最终路线图发布后一年，向总统提供365天状态执行情况报告。此更新将审查整个社区的进度，在切实可行的范围内重新评估威胁，并将讨论来年的关键活动。

正如僵尸网络报告和本文件第二节所讨论的那样，自动化分布式攻击问题无法由一个实体解决，而是需要政府，私营部门（包括行业，学术界和公民社会）。新闻部期待在未来一年及以后与私营部门和其他政府实体合作，改善互联网生态系统的安全性。