NIST Special Publication 800-181

# 全国网络安全教育倡议（NICE）网络安全劳动力框架

翻译人员：樊山 廖宇力

特别鸣谢：贺新朋，以及所有支持本项工作的每一位同仁

William Newhouse

Stephanie Keith

Benjamin Scribner

Greg Witte

本出版物可从 https://doi.org/10.6028/NIST.SP.800-181 免费获取

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-181

# 全国网络安全教育倡议（NICE）网络安全劳动力框架

威廉纽豪斯

*应用网络安全部信息技术实验室*

斯蒂芬妮凯斯

*国防部副首席信息官网络人力战略和政策司办公室*

本杰明 Scribner

*网络教育和意识分支 DHS 国家保护和计划局*

Greg Witte

G2，Inc.安纳波利斯交界处，MD

**本出版物可从 https://doi.org/10.6028/NIST.SP.800-181 免费获取**

August 2017

美国商务部长 Wilbur L. Ross，Jr.秘书

美国国家标准与技术研究院 Kent Rochford，美国国家标准与技术局 NIST 负责人兼商务部副部长

# 目录

# 译者申明

本次翻译工作主要由自由职业者樊山、海南大学廖宇力完成，限于翻译水平及能力问题，文稿中还存在很多瑕疵，诚请各位读者在阅读过程中不吝指正。关于译文中需要说明的几个问题：

1、 译文中有关智力应为情报；

2、 译文在附录中所描述内容没有经过详细审阅，有疑问可与译者联系；

本文原文可在美国 NIST 官方网站下载，本翻译为公益翻译。仅供参考，建议阅读范围：甲方 HR、教育培训部门；乙方 HR、教育培训部门；培训、教育机构以及政策制定方等。

诚请更多爱好者加入这项工作。

邮箱：fanfox7405@163.com 微信号：tianyx74

2018 年 3 月 5 日

# 权威

本出版物由 NIST 根据 2014 年联邦信息安全现代化法案（FISMA）44 美国法令的法定责任制定。§ 3551 及以下，公法（P.L.）113-283。NIST 负责制定信息安全标准和准则，包括对联邦信息系统的最低要求，但这些标准和准则不适用于国家安全系统，未经适当的联邦官员明确批准对这些系统行使政策权限。本指南符合管理和预算局（OMB）A-130 号通告的要求。

本出版物中没有任何内容应该与商务部长根据法定权力制定的强制性和对联邦机构具有约束力的标准和准则相抵触。 这些准则也不应被解释为改变或取代商务部长现任部门，OMB 主任或任何其他联邦官员。 本出版物可能由非政府组织自愿使用，且不受美国版权保护。 但是，NIST 会认可归属。

国家标准与技术研究所 SP 800-181，研究所.站.TECHNOL.规格.公布. 800-181,144 页

（2017 年 8 月）CODEN：NSPUE2 本出版物可从以下网站免费获取：

https：//doi.org/10.6028/NIST.SP.800-181

某些商业实体，设备或材料可能在本文件中被识别以充分描述实验程序或概念。此类标

识并不意味着暗示 NIST 的推荐或认可，也不是意味着实体，材料或设备必定是可用于此目的最佳选择。

本出版物中可能提及 NIST 正根据其分配的法定责任正在开发其他出版物。本出版物中的信息，包括概念和方法，之前由联邦机构使用这些伴随出版物。因此，在每个出版物完成之前，现有的要求，准则和程序仍然有效。出于规划和过渡的目的，联邦机构可能希望密切关注 NIST 发布的这些新出版物。

鼓励组织在公众评议期间审查所有草稿，并向 NIST 提供反馈意见。除上面提到的以外，许多 NIST 网络安全出版物可在 http://csrc.nist.gov/publications 上找到。

**本出版物的评论可能会提交给：**

美国国家标准与技术研究院收件人：NICE，应用网络安全部，信息技术实验室 100 Bureau Drive（Mail Stop 2000）Gaithersburg，MD 20899-2000 电子邮件：ncwf@nist.gov

所有意见均根据信息自由法（FOIA）发布。

# 计算机系统技术报告

NIST 的信息技术实验室（ITL）通过为国家的测量和标准基础设施提供技术领导来促进美国的经济和公共福利。 ITL 开发测试，测试方法，参考数据，概念验证实施和技术分析，以促进信息技术的发展和生产性使用。 ITL 的职责包括制定管理，行政，技术和物理标准以及联邦信息系统中除国家安全相关信息之外的具有成本效益的安全和隐私准则。 SP（特别出版物）800 系列报告了 ITL 在信息系统安全方面的研究，指导方针和推广工作，以及与行业，政府和学术机构的合作活动。

## 摘要

本出版物描述了国家网络安全教育计划（NICE）网络安全劳动力框架（NICE 框架），该框架描述了网络安全工作的跨学科性质。 它是描述和分享网络安全工作信息以及完成任务所需的知识，技能和能力（KSAs）的基本参考资源，可以加强组织的网络安全状态。 作为对网络安全工作进行分类和描述的常用词汇，NICE 框架改善了有关如何识别，招聘，培养和留住网络安全人才的沟通。 NICE 框架是一个参考资料来源，组织或部门可以根据这些资

料开发额外的出版物或工具，以满足他们在网络安全劳动力开发，规划，培训和教育的不同方面界定或提供指导的需求。

## 关键词

能力；网络安全;网络空间；教育；知识；角色；技能；专业领域；任务；训练；工作角色。

## 修订

请访问 NICE 框架修订网站[1]以确定是否有任何对 NICE 框架的更新。

## 补充内容

有关 NICE 框架的参考电子表格，请访问 https://www.nist.gov/file/372581。

## 致谢

作者非常感谢并欣赏个人和组织在公共和私营部门的重要贡献，他们通过深思熟虑提出了建设性意见，提高了本出版物的整体质量，彻底性和实用性。 我们感谢 NIST 的国家网络安全教育计划（NICE）主任 Rodney Petersen 的领导和工作。 我们希望感谢 Tanya Brewer，Dean Bushmiller，Lynne Clarke，Jerri Damavandy，Lisa Dorr，Ryan Farr，Jim Foti，Jodi Guss，Keith Hall，Chris Kelsall，Elizabeth Lennon，Jeff Marron，Joshua Musicante，Stephen Olechnowicz，Lori Pfannenstein，Chuck Romine，Kevin Sanchez-Cherry，Danielle Santos，Stephanie Shively，Matthew Smith，Kevin Stine，Bluma Sussman，Caroline Tan，Baris Yakin 和 Clarence Williams 对本出版物的个人贡献。

第一个 NICE 框架于 2012 年 9 月公布，并于 2013 年 4 月作为国家网络安全工作框架 1.0 版[2]发布。作者承认 Jane Homeyer，Anne Quigley，Rex Min，Noel Kyle，Maya Yankelevich 和 Peggy Maxson 以及蒙大拿威廉姆斯和罗伊伯吉斯在发布于 2014 年 4 月开发国家网络安全劳动力框架 2.0 版中的领导地位 [3]。

最后，作者对计算机安全方面的开创性工作表示敬意，他们的工作可追溯到 20 世纪 60 年代。 计算机安全领域早期先驱者的远见，洞察力和专注努力为本书中提到的任务，知识，

技能和能力提供了哲学和技术基础。

## 商标信息



# 执行摘要

# 1 介绍

国家标准与技术研究院（NIST）在美国商务部领导的全国网络安全教育计划（NICE）中与政府，学术界和私营部门之间是一种伙伴关系，旨在激励和促进强大的网络以及网络安全教育，培训和劳动力发展生态系统。 NICE 通过与政府，学术界和行业合作伙伴进行协调，以现有成功项目为基础，促进变革和创新，并带来领导力和远见，以增加专业网络安全专业人员的数量，从而帮助我们的国家保持安全和经济竞争力。

NICE 致力于培养一支具有全球竞争力的综合性网络安全员工队伍，从聘用到退休，准备好保护我们的国家免受现有和新出现的网络安全挑战。

在整个文档中，“网络安全员工队伍”这个组合术语是对工作角色的简化，这些角色对组织保护其数据，系统和操作的能力有影响。 其中包括传统上被称为信息技术（IT）安全角色的新工作角色。 这些角色已被添加到该员工框架中，以突出其对组织整体网络安全状况的重要性。 此外，本文中描述的一些工作角色包括较短期的网络将包括网络已成为该领域规范的对话领域。

网络安全员工不仅包括以技术为重点的员工，还包括在准备其组织以成功实施其任务时应用网络安全知识的人员。 需要有知识和熟练的网络安全人员来解决组织整体风险管理流程中的网络安全风险。

## 1.1 NICE 框架背景

NICE 框架的概念在 2010 年 NICE 建立之前就开始了，虽然网络安全劳动力还没有明确

规定和评估。 为了应对这一挑战，联邦首席信息官（CIO）理事会在 2008 年接受了任务，为了解联邦政府内的网络安全角色提供了一个标准框架。 来自众多联邦机构的主题专家的焦点小组投入帮助联邦首席信息官委员会编写了一份研究报告，其中提到了其他信息技术专业发展努力已经开始的地方，并且机构确定了进行网络安全工作所需的十三种具体作用。

在对网络安全“领域”内进行多学科探索的基础上，全面的国家网络安全倡议包括将工作重点放在若干机构的共同努力下开发网络安全工作人员框架。 第一稿于 2011 年 9 月发布，征询公众意见。审核已纳入 1.0 版[2]。

随后美国政府范围审查指出具体领域需要进一步审查和完善。 国土安全部（DHS）通过汇集焦点小组与来自全国各地以及行业，学术界和政府的主题专家投入并验证了最终建议，生成第二版 NICE 框架 2.0 版[3]，并与 2014 年公开发布共享。

国防部长办公室（OSD）通过与服务部门的内部合作以及与私营部门的外部合作扩展了 2.0 版本。美国国土安全部和 NIST 的共同作者与 OSD 合作，完善并扩展成为本出版物，其目标是强调私营部门的适用性，并强化 NICE 框架是公共和私营部门参考资源的愿景。

## 1.2 目的和适用性

本出版物是支持能够满足组织网络安全需求的员工的基本参考资源。 它为组织提供了一个共同的，一致的词典来对网络安全工作进行分类和描述。

使用 NICE 框架作为基本参考将改善识别，招聘和培养网络安全人才所需的沟通。 NICE 框架将允许雇主在专业发展计划中使用专注一致的语言，使用行业认证和学历证书，并为其员工选择相关的培训机会。

NICE 框架有助于使用更一致，可比较和可重复的方法为组织内职位选择和指定网络安全角色。 它还提供了一个通用的词汇，学术机构可以用它来开发网络安全课程，更好地为学生提供当前和预期的网络安全人员需求。

NICE 框架的应用提供描述所有网络安全工作的能力。 NICE 框架的适用性目标是任何网络安全工作或职位都可以通过识别来自 NICE 框架的一个或多个组件的相关材料来描述。对于每个工作或职位，任务或业务流程的背景和优先级将推动从 NICE 框架中选择哪些材料。

组织或部门可以使用 NICE 框架来开发额外的出版物或工具，以满足他们的需求，以定义或提供劳动力发展，规划，培训和教育的不同方面的指导。

## 1.3 受众和用户

NICE 框架可以被视为非规范性的网络安全劳动力词典。 NICE 框架的参考用户应该在本地实施不同的劳动力发展，教育或培训为目的。

### 1.3.1 雇主

使用 NICE 框架的通用词典使雇主能够盘点和发展他们的网络安全人员队伍。 NICE 框架可以被雇主和组织领导用来：

- 盘点并跟踪他们的网络安全人员，以更好地了解所执行的知识，技能，能力和任务的优势和差距;
- 确定培训和资格要求，以开发关键的知识，技能和能力来执行网络安全任务;
- 一旦确定工作角色和任务，改进职位说明和职位空缺通知，选择相关的 KSA 和任务;
- 确定最相关的工作角色并制定职业路径，以指导员工获得这些角色所需的技能; 和
- 在招聘经理和人力资源（HR）员工之间建立共同的术语，以招聘，保留和培训高度专业化的员工队伍。

### 1.3.2 当前和未来的网络安全工作者

NICE 框架支持网络安全领域的人员以及那些可能希望进入网络安全领域的人员，以探索网络安全类别和工作角色中的任务。 它还协助那些支持这些工作者的人员，如人力资源配备专家和指导顾问，帮助求职者和学生了解哪些网络安全工作的作用以及哪些相关的知识，技能和能力正在被雇主重视，用于未定义的网络安全工作和职位。

当空缺通知和开放职位描述使用 NICE 框架的通用词典对网络安全任务和这些职位所需的培训提供清晰一致的描述时，这些工作人员得到进一步支持。

当培训提供商和行业认证提供商使用 NICE 框架的通用词典时，网络安全领域的人员或可能希望进入网络安全领域的人员可以找到培训和/或认证提供者，以便教授必要的任务以确保 网络安全工作或进入新职位。使用通用词典可帮助学生和专业人员获得 KSA，这些 KSA 通常由网络安全职位包含特定工作角色的人员进行演示。 这种理解有助于他们找到包含学习成果和知识单位的学术课程，这些单元可映射到由雇主评估的 KSA 和任务。

### 1.3.3 教育者/培训者

NICE 框架为教育工作者提供了一个参考资料，用于开发涵盖 NICE 框架中描述的 KSA 和任务的课程，证书或学位课程，培训课程，课程，研讨会，训练或挑战。

人力资源人员配置专家和辅导员可以使用 NICE 框架作为职业探索的资源。

### 1.3.4 技术提供者

NICE 框架允许技术提供商识别与他们提供的硬件和软件产品及服务相关的网络安全工作角色以及 KSA 和任务。 然后，技术提供商可以创建适当的支持材料，协助网络安全人员对其产品进行适当的配置和管理。

## 1.4 这个特别出版物的组织

本特别出版物的其余部分安排如下：

- 第 2 章定义了 NICE 框架的组成部分：（i）分类；（ii）专业领域；（iii）工作角色；（iv）相关的知识，技能和能力及每个工作角色的任务。
- 第 3 章介绍如何使用 NICE 框架
- 第 4 章指出了其他出版物，指导方针，指南和工具可以扩大 NICE 框架影响的领域。
- 附录 A 描述了 NICE 框架的类别，专业领域，工作角色，KSA 和任务清单。
- 附录 B 提供了每个工作角色的详细列表，包括相关的 KSA 和任务。
- 附录 C 提供了一些劳动力开发工具的例子
- 附录 D 提供了指南或指南文件的一些例子，它们将这些文件的一些内容交叉引用到 NICE 框架中的组件
- 附录 E 给出了本文档中使用的选定首字母缩略词和缩写。
- 附录 F 给出了本文引用的参考文献。

# 2 NICE 框架组件和关系

## 2.1 NICE 框架的组成部分

NICE 框架组织网络安全和相关工作。 本节介绍并定义 NICE 框架的核心组件，以支持这些领域。

### 2.1.1 类别

类别提供了 NICE 框架的总体组织结构。 有七个类别，全部由专业领域和工作角色组成。 这种组织结构基于广泛的工作分析，它将具有共同主要职能的工作人员和工作组织在一起，无论职位或其他职业条款如何。

### 2.1.2 专业领域

类别包含网络安全工作分组，称为专业领域。 在国家网络安全劳动力框架 1.0 版中有 31 个专业领域[2]，国家网络安全工作框架 2.0 版中有 32 个[3]。 每个专业领域都是网络安全和相关工作中集中工作或功能的领域。 在以前版本的 NICE 框架中，任务和 KSA 与每个专业领域相关联。 KSA 和任务现在与工作角色相关联。

### 2.1.3 工作角色

工作角色是网络安全和相关工作中最详细的组合，其中包括以知识，技能和能力（KSA）形式履行角色所需的属性列表以及在该角色中执行的任务。

通过从 NICE 框架中选择与该工作或职位相关的一个或多个工作角色来描述在工作或职位上执行的工作，以支持任务或业务流程。

为了协助组织和沟通有关网络安全责任，工作角色分为特定类别和专业领域，如附录 A 所示。

### 2.1.4 知识、技能和能力 (KSAs)

知识，技能和能力（KSAs）是执行工作角色所需要的属性，通常通过相关的经验，教育

或培训来证明。

- 知识是直接应用于功能表现的一组信息。
- 技能通常被定义为执行可观察到的学习型心理行为的能力。 心理领域的技能描述了物理操纵工具或手段的能力，如手或锤子。 网络安全所需的技能应该少依赖于对工具和工具的物理操纵，更多地依靠对组织或个人的网络安全状况产生影响的工具，框架，流程和控制。
- 能力是执行可观察行为或导致可观察到产品行为的能力。

### 2.1.5 任务

任务是一项具体定义的工作，与其他确定的任务相结合，组成了特定专业领域或工作角色的工作。

## 2.2 NICE 框架组件关系

NICE 框架组件描述了网络安全工作。 如图 1 所示，每个类别都由专业领域组成，每个专业领域都由一个或多个工作角色组成。 每个工作角色又包括 KSA 和任务。

以这种方式对组件进行分组可简化有关网络安全劳动力主题的交流，并有助于与其他框架保持一致。 附录 B 和在 NICE 框架网站[5]上发布的参考电子表格[4]中显示了特定的工作角色与 KSA 和任务的关联。

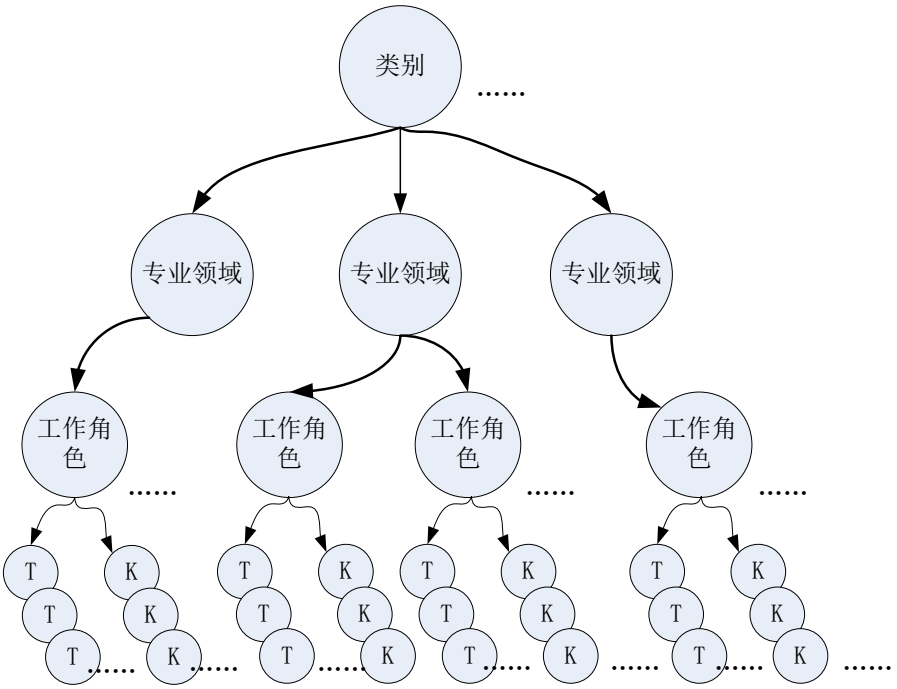


图 1 – NICE 框架组件之间的关系

# 3 使用 NICE 框架

使用 NICE 框架了解组织需求并评估满足这些需求的程度可以帮助组织规划，实施和监控成功的网络安全计划。

## 3.1 确定网络安全劳动力需求

网络安全是一个迅速变化和扩大的领域。 这种扩张需要一批熟练的工作人员来帮助组织履行网络安全职能。 随着组织确定需要什么来充分管理当前和未来的网络安全风险，领导者需要考虑网络安全人员的能力和所需的能力。

图 2 展示了 NICE 框架如何成为帮助雇主建立一支有能力并且准备好的网络安全人员队伍的中心参考。

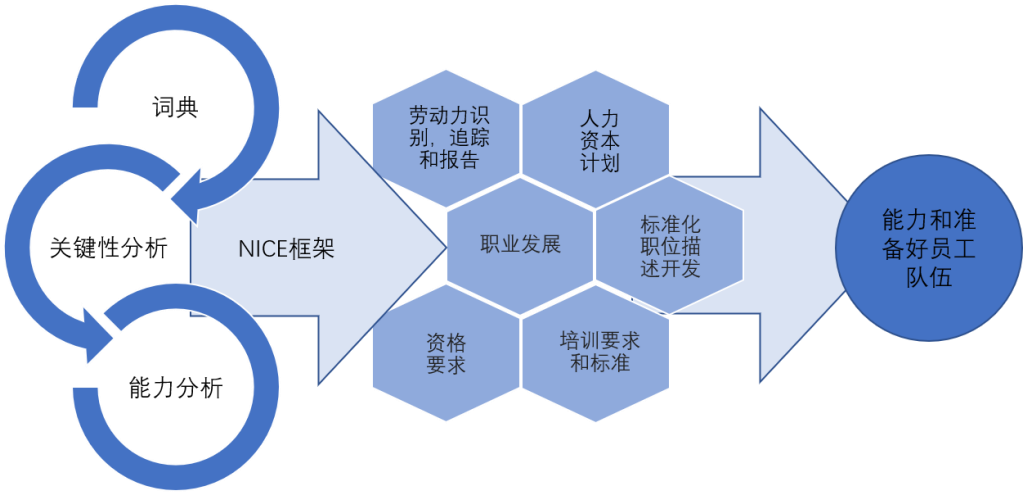


图 2 – 为有能力和准备好的网络安全人员提供构建模块

图 2 左侧的圆形箭头表示可能会影响组织开发有能力且随时准备就绪的员工的能力：

- 使用 NICE 框架的通用词汇表澄清网络安全教育者，培训者/认证者，雇主和雇员之间的沟通。
- 执行关键性分析将识别对于具有给定工作角色的成功绩效和对于多个工作角色而言关键的 KSA 和任务。
- 运行能力程度分析将通知组织对期望职位（例如入门级，专家）的期望，职位通常由多个工作角色组成。 熟练程度分析应该能够完善相关任务的选择，而 KSA 则是组成该职位的工作角色所需要的。

附录 C 列出了一些支持识别网络安全劳动力需求的现有劳动力开发工具。

## 3.2 高技能网络安全人才的招聘和录用

参考 NICE 框架将帮助企业完成战略性人力资源规划和招聘。 NICE 框架材料在创建或修改职位空缺通知和招聘岗位描述时将用于帮助候选人寻找他们感兴趣，有能力或有资格的特定职位。 用于描述职位职责和责任的任务以及用于描述岗位所需技能和资格的 KSA 应允许候选人和招聘经理更有效地沟通。 使用 NICE 框架术语的职位描述和职位空缺公告支持审核候选人的更一致的评估标准。

对于关注员工差距的组织，审核 NICE 框架的任务列表可以确定组织未执行的具体任务。这些任务允许组织确定差距的工作角色和专业领域。组织能够更好地提供教育，培训和认证以及将其产品映射到 NICE 框架与社区进行交流。 该组织可以确定将允许现有工作人员解

决差距的培训。组织的招聘经理使用这种方式从 NICE 框架提取的数据，可以识别拥有 KSAs 的申请人执行网络安全任务。

## 3.3 网络安全劳动力成员的教育和培训

NICE 框架确定工作角色中的任务可能使教育工作者为学习者准备具体的 KSA，他们可以从中展示执行网络安全任务的能力。

学术机构是准备和教育网络安全人员的关键部分。 公共和私人实体之间的合作，例如通过 NICE 计划，使这些机构能够确定所需的共同知识和能力。 反过来，制定和提供与 NICE 框架词汇相一致的课程，使机构能够为学生提供雇主所需的技能。 随着网络安全领域寻找期望工作的学生人数增加，越来越多的学生将被吸引到学术网络安全计划中作为职业发展的途径。

## 3.4 高技能网络安全人才的保留与发展

熟练的网络安全人员的一个关键方面是发展和保留已经加入的熟练人才。当前的员工拥有难以取代的现有关系，机构知识和组织经验。 员工离职后重新填补职位可能会带来新的广告和招聘成本，培训费用，生产力下降以及士气下降。 以下列表说明了 NICE 框架支持保留和发展网络安全人才的一些方式：

- 组织可以开发职业途径，描述日益具有挑战性和不断发展的工作角色所需的资格，例如 NICE 框架列举的那些角色。
- 对 KSAs 和任务的详细了解有助于现有员工了解发展其能力所需的具体步骤，以促进准备就绪。
- 一个组织可能会提供轮换工作人员以提供开发和使用新技能的机会。
- 组织可以确定在相关领域努力改进 KSAs 的人员，认识那些表现良好的人员。
- 组织可以为员工制定发展/改进计划，帮助他们制定出他们如何获得新工作角色所需的 KSA。
- 可以确定集体培训机会，以使员工为组织的工作角色提高共同知识，技能和能力做好准备。
- 组织可以使用基于特定网络安全技能和能力的培训和考试来评估现实环境中的熟练程度。

- 组织可以利用现有人员填补关键的网络安全人员需求，利用审查现有员工简历的能力来识别具有理想 KSA 的人员。
- NICE 框架对希望从其他职位转入网络安全工作角色的现有员工有所帮助。一个组织可以描述需要的 KSA，以使非网络安全工作角色的可靠员工成为网络安全工作人员的一部分，从事网络安全任务。

# 4 扩展

组织或部门可以使用 NICE 框架来开发额外的出版物或工具来满足他们的需求，并定义或提供劳动力发展，规划，培训和教育的不同方面的指导。

NICE 框架中交叉引用元素的新参考资料将通过 NICE 网站共享[5]。

以下几个领域是可以开发其他出版物或工具的几个例子。

## 4.1 能力

劳动部就业和培训管理局[6]将能力定义为能够运用或使用知识，技能，能力，行为和个人特征成功完成关键工作任务，特定职能或在特定角色或职位上工作。 除了列举技术 KSAs 外，能力模型还考虑行为指标并描述非技术性考虑因素，例如个人效能，学术和工作场所能力。 关于这些考虑因素的更多信息可以从劳工部的 CareerOneStop 站点获得[7]。

## 4.2 职位名称

职位名称是对员工在组织中的工作或职位的描述。 将样本职位名称映射到专业领域或工作角色将有助于组织使用 NICE 框架。

## 4.3 网络安全指南和指南文件

NICE 战略目标 3，指导职业发展和劳动力规划，旨在支持雇主应对市场需求并加强网络安全人才的招聘，聘用，发展和留用。 这个战略目标的一个目标是发布和提高 NICE 框架的意识并鼓励采用。 在这种情况下的采用意味着 NICE 框架被用作与网络安全人员，培训和教育相关的行动的参考资源。

鼓励采用NICE框架的一种方式是鼓励网络安全指南或指南文档的作者将其内容与NICE框架的组件交叉引用。 附录D探讨了三个示例出版物。

# 附录 A – NICE 框架元素列表

## A.1 NICE 框架劳动力类别

表 1 提供了 NICE 框架描述的每个类别的描述。 每个都包含一个两字符的缩写（例如SP），用于快速参考该类别并支持创建NICE框架工作角色标识符（请参阅表 3 - NICE框架工作角色）。 此列表将定期更新[1]。 NIST特别出版物800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 1 - NICE 框架劳动力类别**

| 类别 | 描述 |
|---|---|
| 安全准备（SP） | 概念化，设计，采购和/或构建安全信息技术（IT）系统，并负责系统和/或网络开发的各个方面。 |
| 操作和维护（OM） | 提供确保有效和高效的信息技术（IT）系统性能和安全所需的支持，管理和维护。 |
| 监督和治理（OV） | 提供领导，管理，指导，发展和倡导能力，以便组织可以有效地开展网络安全工作。 |
| 保护和防御（PR） | 识别，分析和减轻内部信息技术（IT）系统和/或网络的威胁。 |
| 分析（AN） | 对传入的网络安全信息进行高度专业化的审查和评估，以确定其对情报的有用性。 |
| 收集和操作（CO） | 提供专门的拒绝和欺骗操作技能，并收集可用于开发情报的网络安全信息。 |
| 调查（IN） | 调查与信息技术（IT）系统，网络和数字证据相关的网络安全事件或犯罪。 |

## A.2 NICE 框架专业领域

表2提供了每个NICE框架专业领域的描述。 每个专业领域都包含一个三字符缩写（例

如 RSK），以便快速参考专业领域并支持创建 NICE 框架工作角色标识符（请参阅表 3 - NICE 框架工作角色）。 此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 2 - NICE 框架专业领域**

| 分类 | 专业领域 | 专业领域描述 |
|---|---|---|
| 安全准备（SP） | 风险管理（RSK） | 监督，评估和支持必要的文档，验证，评估和授权过程，以确保现有的和新的信息技术（IT）系统满足组织的网络安全和风险要求。 从内部和外部角度确保风险，合规性和保证的适当处理。 |
| | 软件开发（DEV） | 根据软件保证最佳实践开发和编写/编码新（或修改现有）计算机应用程序，软件或专用实用程序。 |
| | 系统架构（ARC） | 开发系统概念及开发系统开发生命周期的功能阶段； 将技术和环境条件（例如法律和法规）转化为系统和安全设计和流程。 |
| | 技术研发（TRD） | 进行技术评估和整合过程； 提供并支持原型能力和/或评估其效用。 |
| | 系统需求规划（SRP） | 与客户协商收集和评估功能需求，并将这些需求转化为技术解决方案。 为客户提供有关信息系统适用性的指导以满足业务需求。 |
| | 测试和评估（TST） | 开发和实施系统测试，通过应用成本效益计划，评估，验证和验证技术，功能和性能特征（包括互操作性）系统或包含 IT 的系统元素的原则和方法来评估符合规范和要求的情况。 |
| | 系统开发（SYS） | 在系统开发生命周期的开发阶段工作。 |
| 操作和维护（OM） | 数据管理（DTA） | 开发和管理允许存储，查询，保护和使用数 |

| | | |
|---|---|---|
| | | 据的数据库和/或数据管理系统。 |
| | 知识管理（KMG） | 管理和管理流程及工具，使组织能够识别，记录和访问知识资本和信息内容。 |
| | 客户服务和技术支持（STS） | 解决安装，配置，排除故障问题并根据客户要求提供查询维护和培训（例如，分级客户支持）。 通常为事件响应（IR）专业提供初始事件信息。 |
| | 网络服务（NET） | 安装，配置，测试，操作，维护和管理网络及其防火墙，包括硬件（例如集线器，网桥，交换机，多路复用器，路由器，电缆，代理服务器和保护性分配器系统）以及允许共享和传输的软件所有系列传输信息来支持信息和信息系统的安全。 |
| | 系统管理（ADM） | 安装，配置，排除故障并维护服务器配置（硬件和软件）以确保其机密性，完整性和可用性。 管理帐户，防火墙和补丁。 负责访问控制，密码以及帐户创建和管理。 |
| | 系统分析（ANA） | 研究一个组织当前的计算机系统和程序，并设计信息系统解决方案，以帮助组织更安全，高效和有效地运作。 通过了解两者的需求和局限，将业务和信息技术（IT）融合在一起。 |
| 监督和治理（OV） | 法律咨询和倡导（LGA） | 向领导层和员工就各种相关主题领域内提供合法的意见和建议。 宣扬法律和政策变更，并通过各种书面和口头工作产品代表客户提起诉讼，包括法律简报和诉讼程序。 |
| | 培训、教育和意识（TEA） | 在相关学科领域内进行人员培训。 酌情制定，计划，协调，交付和/或评估培训课程，方法和技术。 |

| | | |
|---|---|---|
| | 网络安全管理（MGT） | 监督信息系统或网络的网络安全计划，包括管理组织内部的信息安全影响，特定计划或其他责任领域，包括战略，人员，基础设施，要求，政策执行，应急计划，安全意识和其他资源。 |
| | 战略规划和策略（SPP） | 制定政策和计划和/或倡导改变支持组织网络空间举措或需要改变/增强的政策。 |
| | 执行网络领导（EXL） | 监督，管理和/或领导执行网络和网络相关和/或网络运营工作的工作人员。 |
| | 计划/项目管理（PMA）和收购 | 应用数据，信息，流程，组织交互，技能和分析专业知识以及系统，网络和信息交换能力的知识来管理采购项目。 执行管理硬件，软件和信息系统采购计划和其他计划管理政策的职责。为采用信息技术（IT）（包括国家安全系统）的采购提供直接支持，应用与 IT 相关的法律和政策，并在整个采购生命周期中提供与 IT 相关的指导。 |
| 保护和防御（PR） | 网络防御分析（CDA） | 使用从各种来源收集的防御措施和信息来识别，分析和报告网络中发生或可能发生的事件，以保护信息，信息系统和网络免受威胁。 |
| | 网络防御基础设施支持（INF） | 测试，实施，部署，维护，审查和管理有效管理计算机网络防御服务提供商网络和资源所需的基础架构硬件和软件。监控网络以主动修复未经授权的活动。 |
| | 事件响应（CIR） | 应对相关领域内的危机或紧急情况，以缓解直接和潜在的威胁。根据需要使用缓解，准备以及响应和恢复方法，以最大限度地提高生存期，财产保全和信息安全。调查并 |

| | | |
|---|---|---|
| | | 分析所有相关的响应活动。 |
| | 漏洞评估和管理（VAM） | 对威胁和脆弱性进行评估;确定与可接受配置，企业或当地政策的偏差;评估风险水平;并在运营和非运营情况下制定和/或建议适当的缓解对策。 |
| 分析（AN） | 威胁分析（TWA） | 识别和评估网络安全罪犯或外国情报机构的能力和活动； 产生调查结果以帮助初始化或支持执法和反间谍调查或活动。 |
| | 开发分析（EXP） | 分析收集到的信息以识别漏洞和潜在的利用。 |
| | 全源分析（ASA） | 分析情报社区中多个来源，学科和机构的威胁信息。在情境中合成和放置情报信息;吸取关于可能产生影响的见解。 |
| | 目标（TGT） | 应用当前对一个或多个地区，国家，非国家实体和/或技术的了解。 |
| | 语言分析（LNG） | 应用语言，文化和技术专业知识来支持信息收集，分析和其他网络安全活动。 |
| 收集和操作（CO） | 收集操作（CLO） | 使用适当的策略并在通过收集管理流程确定的优先级内执行收集。 |
| | 网络运营计划（OPL） | 执行深入的联合目标和网络安全规划过程。 收集信息并制定详细的操作计划和订单支持要求。 针对综合信息和网络空间作战的全部业务执行战略和业务层面的规划。 |
| | 网络运营（OPS） | 执行活动收集犯罪或外国情报实体的证据，以缓解可能的或实时的威胁，防止间谍活动或内部威胁，外国破坏活动，国际恐怖主义活动或支持其他情报活动。 |
| 调查（IN） | 网络调查（INV） | 全面的调查工具和流程应用策略，技巧和 |

| | | |
|---|---|---|
| | | 程序，包括但不限于访谈和询问技巧，监视，反监视和监视检测，并适当平衡起诉与情报收集的益处。 |
| | 数字取证（FOR） | 收集，处理，保存，分析和提供计算机相关证据，以支持网络漏洞缓解和/或犯罪，欺诈，反间谍或执法调查。 |

## A.3 NICE 框架工作角色

表 3 提供了 NICE 框架描述的每个工作角色的描述。 每个工作角色由类别和专业领域确定，然后是序列号（例如，SP-RSK-001 是 SP 类别和 RSK 专业领域中的第一个工作角色）。部分工作角色说明来源于外部文件（例如国家安全系统指令委员会[CNSSI] 4009），并将该信息包含在说明栏中。 此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

表 3 - NICE 框架工作角色

| 类别 | 专业领域 | 工作角色 | 工作角色 ID | 工作角色描述 |
|---|---|---|---|---|
| 安全准备（SP） | 风险管理（RSK） | 授权官员/指定代表 | SP-RSK-001 | 高级官员或执行官，有权正式承担在组织运营（包括任务，职能，形象或声誉），组织资产，个人，其他组织和国家可接受的风险水平下运营信息系统的责任（CNSSI 4009）。 |
| | | 安全控制评估员 | SP-RSK-002 | 对信息技术（IT）系统内部采用或继承的管理，运营和技术安全控制和增强控制进行独立综合评估，以确定控制的整体有效性（如 NIST SP 800-37 中所定义）。 |
| | 软件开发（DEV） | 软件开发人员 | SP-DEV-001 | 开发，创建，维护和编写/编码新的（或修改现有的）计算机应用程序，软件或专用实用程序。 |
| | | 安全的软件评估 | SP-DEV-002 | 分析新的或现有的计算机应用程序，软件或专用实用程序的安全性并提供可操作的结果。 |
| | 系统架构（ARC） | 企业架构师 | SP-ARC-001 | 开发并维护业务，系统和信息流程以支持企业任务需求；开发描述基线和目标体系结构的信息技术（IT）规则和要求。 |
| | | 安全架构师 | SP-ARC-002 | 确保在企业架构的所有方面（包括参考模型，细分市场和解决方案架构以及支持这些任务和业务流程的最终系统）充分解决保护组织的使命和业务流程所需的利益相关方安全需求。 |

| | | | | |
|---|---|---|---|---|
| | 技术研发（TRD） | 研究和开发专家 | SP-TRD-001 | 开展软件和系统工程和软件系统研究，开发新功能，确保网络安全完全整合。开展全面的技术研究，以评估网络空间系统的潜在脆弱性。 |
| | 系统需求规划（SRP） | 系统需求规划员 | SP-SRP-001 | 咨询客户以评估功能需求并将功能需求转化为技术解决方案。 |
| | 测试和评估（TST） | 系统测试和评估专家 | SP-TST-001 | 计划，准备并执行系统测试，根据规格和要求评估结果，并分析/报告测试结果。 |
| | 系统开发（SYS） | 信息系统安全开发者 | SP-SYS-001 | 在整个系统开发生命周期中设计，开发，测试和评估信息系统安全。 |
| | | 系统开发者 | SP-SYS-002 | 在整个系统开发生命周期中设计，开发，测试和评估信息系统。 |
| 操作和维护（OM） | 数据管理（DTA） | 数据库管理员 | OM-DTA-001 | 管理允许安全存储，查询，保护和使用数据的数据库和/或数据管理系统。 |
| | | 数据分析师 | OM-DTA-002 | 检查来自多个不同来源的数据，以提供安全和隐私洞察力。 设计并实现用于建模，数据挖掘和研究目的的复杂企业级数据集的自定义算法，工作流程和布局。 |
| | 知识管理（KMG） | 知识经理 | OM-KMG-001 | 负责流程和工具的管理和管理，使组织能够识别，记录和访问智力资本和信息内容。 |
| | 客户服务和技术支持（STS） | 技术支持专家 | OM-STS-001 | 根据既定或批准的组织过程组件（即适用的主事件管理计划），为需要使用客户级硬件和软件的客户提供技术支持。 |

| | | | | |
|---|---|---|---|---|
| | 网络服务（NET） | 网络运营专家 | OM-NET-001 | 计划，实施和运营网络服务/系统，包括硬件和虚拟环境。 |
| | 系统管理（ADM） | 系统管理员 | OM-ADM-001 | 负责设置和维护系统或系统的特定组件（例如，安装，配置和更新硬件和软件;建立和管理用户帐户;监督或执行备份和恢复任务;实施操作和技术安全控制;并遵守组织安全政策和程序）。 |
| | 系统分析（ANA） | 系统安全分析师 | OM-ANA-001 | 负责分析和开发系统安全的集成，测试，操作和维护。 |
| 监督和治理（OV） | 法律咨询和倡导（LGA） | 网络法律顾问 | OV-LGA-001 | 就网络法相关主题提供法律咨询和建议。 |
| | | 隐私官/隐私合规经理 | OV-LGA-002 | 开发和监督隐私合规计划和隐私计划人员，支持隐私和安全管理人员及其团队的隐私合规性，治理/政策和事件响应需求。 |
| | 培训，教育和意识（TEA） | 网络教育课程开发者 | OV-TEA-001 | 根据教学需求开发，计划，协调和评估网络培训/教育课程，方法和技术。 |
| | | 网络教师 | OV-TEA-002 | 开发并开展网络领域内人员的培训或教育。 |
| | 网络安全管理（MGT） | 信息系统安全经理 | OV-MGT-001 | 负责项目，组织，系统或飞地的网络安全。 |
| | | 通信安全（COMSEC）经理 | OV-MGT-002 | 管理组织通信安全（COMSEC）资源的个人（CNSSI 4009）或加密密钥管理系统（CKMS）的密钥管理员。 |
| | 战略规划与政策（SPP） | 网络劳动力开发人员和经理 | OV-SPP-001 | 制定网络空间劳动力计划，战略和指导，以支持网络空间劳动力的人力，人员，培训和教育需求，并解决网络空间政策，原则，物资，部队结构以及教育和培训要求的变化。 |

| | | | | |
|---|---|---|---|---|
| | | 网络政策和策略规划 | OV-SPP-002 | 制定和维护网络安全计划，战略和政策，以支持和协调组织网络安全举措和法规遵从。 |
| | 行政网络领导力（EXL） | 行政网络领导 | OV-EXL-001 | 执行决策权并为组织的网络和网络相关资源和/或运营确定愿景和方向。 |
| | | 项目经理 | OV-PMA-001 | 计划/项目管理（PMA）和收购<br>领导，协调，沟通，整合，并对项目的整体成功负责，确保与机构或企业优先事项保持一致。 |
| | | IT 项目经理 | OV-PMA-002 | 直接管理信息技术项目。 |
| | | 产品支持经理 | OV-PMA-003 | 管理现场所需的一揽子支持功能，并保持系统和组件的准备就绪和运营能力。 |
| | | IT 投资/投资组合经理 | OV-PMA-004 | 管理符合特派团和企业优先事项总体需求的 IT 投资组合。 |
| | | IT 计划审计员 | OV-PMA-005 | 对 IT 计划或其各个组件进行评估，以确定是否符合公布的标准 |
| 保护和防御（PR） | 网络防御分析（CDA） | 网络防御分析师 | PR-CDA-001 | 使用从各种网络防御工具（例如 IDS 警报，防火墙，网络流量日志）收集的数据来分析其环境中发生的事件，以减轻威胁。 |
| | 网络防御基础设施支持（INF） | 网络防御基础架构支持专家 | PR-INF-001 | 测试，实施，部署，维护和管理基础架构硬件和软件。 |
| | 事件响应（CIR） | 网络防御事件响应 | PR-CIR-001 | 调查，分析并响应网络环境或飞地内的网络事件。 |

| | | | | |
|---|---|---|---|---|
| | | 者 | | |
| | 漏洞评估和管理（VAM） | 漏洞评估分析师 | PR-VAM-001 | 对网络环境或飞地内的系统和网络进行评估，并确定这些系统/网络偏离可接受配置，飞地策略或本地策略的位置。衡量深度防御架构针对已知漏洞的有效性。 |
| 分析（AN） | 威胁分析（TWA） | 威胁/警告分析师 | AN-TWA-001 | 开发网络指标以保持对高度动态运行环境状态的认识。收集，处理，分析和传播网络威胁/警告评估。 |
| | 开发分析（EXP） | 开发分析师 | AN-EXP-001 | 合作确定通过网络收集和/或准备活动可以满足的访问和收集差距。利用所有授权资源和分析技术来渗透目标网络。 |
| | 全源分析（ASA） | 全源分析师 | AN-ASA-001 | 分析来自一个或多个来源的数据/信息，以开展环境准备，响应信息请求，并提交情报收集和生产要求以支持规划和运营。 |
| | | 任务评估专家 | AN-ASA-002 | 制定评估计划和绩效/有效性措施。根据网络活动的要求进行战略和运营效果评估。确定系统是否按预期执行，并为确定运营有效性提供输入。 |
| | 目标（TGT） | 目标开发者 | AN-TGT-001 | 执行目标系统分析，构建和/或维护电子目标文件夹，以包括来自环境准备和/或内部或外部情报源的输入。与合作伙伴目标活动和情报组织协调，并提出候选目标进行审查和验证。 |
| | | 目标网络分析师 | AN-TGT-002 | 对收集和开源数据进行高级分析，以确保目标的连续性;分析目标及其活动;并开发获取更多目标信息的技术。根据对目标技术，数字网络及其应用 |

| | | | | |
|---|---|---|---|---|
| | | | | 程序的了解，确定目标如何进行通信，移动，操作和生活。 |
| | 语言分析（LNG） | 多学科语言分析师 | AN-LNG-001 | 应用具有目标/威胁和技术知识的语言和文化专业知识来处理，分析和/或传播从语言，语音和/或图形资料中获取的情报信息。创建并维护特定语言的数据库和工作辅助工具，以支持网络行动执行并确保关键知识共享。提供外语密集或跨学科项目的主题专业知识。 |
| 收集和操作（CO） | 收集操作（CLO） | 全源收集经理 | CO-CLO-001 | 确定收集当局和环境;将优先信息要求纳入收集管理;开发符合领导意图的概念。确定可用收集资产的能力，确定新的收集能力;并构建和传播收集计划。监控任务收集的执行情况，以确保收集计划的有效执行。 |
| | | 全源收集需求管理者 | CO-CLO-002 | 评估收集操作并开发基于效果的收集需求策略，使用可用的来源和方法来改进收集。开发，处理，验证和协调收集要求的提交。评估收集资产和收集操作的性能。 |
| | 网络运营规划（OPL） | 网络 Intel 规划 | CO-OPL-001 | 制定详细的情报计划，以满足网络作战要求。与网络运营规划人员合作确定，验证和征收收集和分析要求。参与网络行动的选择，验证，同步和执行。同步情报活动以支持网络空间中的组织目标。 |
| | | 网络运营规划 | CO-OPL-002 | 通过与其他计划者，运营商和/或分析师的合作，制定详细的计划，以管理或支持适用范围的网络运营。参与瞄准选择，验证，同步，并在网络行动执行期间实现整合。 |

| | | | | |
|---|---|---|---|---|
| | | 合作伙伴集成规划员 | CO-OPL-003 | 致力于推动网络运营合作伙伴之间跨组织或国家边界的合作。通过提供指导，资源和协作来帮助合作伙伴网络团队的整合，以发展最佳实践并促进组织对实现综合网络行动目标的支持。 |
| | 网络运营（OPS） | 网络运营商 | CO-OPS-001 | 进行系统的收集，处理和/或地理定位以利用，定位和/或跟踪感兴趣的目标。 执行网络导航，战术取证分析，并在执行网络操作时执行。 |
| 调查（IN） | 网络调查（INV） | 网络犯罪调查员 | IN-INV-001 | 使用受控和记录的分析和调查技术识别，收集，检查和保存证据。 |
| | 数字取证（FOR） | 执法/反间谍取证分析师 | IN-FOR-001 | 对基于计算机的犯罪行为进行详细调查，建立文件或物证，包括与网络入侵事件相关的数字媒体和日志。 |
| | | 网络防御取证分析师 | IN-FOR-002 | 分析数字证据并调查计算机安全事件以获取有用的信息,以支持系统/网络漏洞缓解。 |

## A.4 NICE 框架任务

表 4 列出了所有已确定为网络安全工作角色的任务。 每个工作角色都包含此处列出的任务的一个子集。 此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 4 - NICE 框架任务**

| 任务 ID | 描述 |
|---|---|
| T0001 | 获取和管理必要的资源，包括领导支持，财务资源和关键安全人员，以支持信息技术（IT）安全目标和目的，并降低整体组织风险。 |
| T0002 | 获得必要的资源，包括财务资源，以实施有效的企业运营计划连续性。 |
| T0003 | 就风险水平和安全状况向高级管理层（如首席信息官[CIO]）提供建议。 |
| T0004 | 就信息安全计划，政策，流程，系统和要素的成本/收益分析向高级管理层（如 CIO）提供建议。 |
| T0005 | 向适当的高层领导或授权官员咨询影响组织网络安全态势的变化。 |
| T0006 | 倡导组织在法律和立法程序中的官方立场。 |
| T0007 | 分析和定义数据要求和规格。 |
| T0008 | 分析和规划数据容量需求的预期变化。 |
| T0009 | 分析信息以确定，推荐和规划新应用程序的开发或现有应用程序的修改。 |
| T0010 | 分析组织的网络防御政策和配置，并评估对法规和组织指令的遵守情况。 |
| T0011 | 分析用户需求和软件需求，以确定在时间和成本约束下设计的可行性。 |
| T0012 | 分析设计约束，分析权衡，详细的系统和安全设计，并考虑生命周期支持。 |
| T0013 | 应用编码和测试标准，应用包括“模糊测试”静态分析代码扫描工具在内的安全测试工具，并进行代码审查。 |
| T0014 | 应用安全的代码文档。 |
| T0015 | 将安全策略应用于彼此交互的应用程序，如企业对企业（B2B）应用程序。 |
| T0016 | 应用安全策略来满足系统的安全目标。 |

| | |
|---|---|
| T0017 | 应用面向服务的安全体系结构原则来满足组织的机密性，完整性和可用性要求。 |
| T0018 | 评估系统使用的网络安全措施的有效性。 |
| T0019 | 评估计算机系统的威胁和漏洞以制定安全风险概况。 |
| T0020 | 为网络防御工具开发内容。 |
| T0021 | 使用工作模型或理论模型构建，测试和修改产品原型。 |
| T0022 | 捕获需求阶段使用的安全控制，将安全性集成到流程中，识别关键安全性目标，最大限度地提高软件安全性，同时最大限度地减少对计划和计划的干扰。 |
| T0023 | 表征和分析网络流量以识别异常活动和对网络资源的潜在威胁。 |
| T0024 | 收集和维护满足系统网络安全报告所需的数据。 |
| T0025 | 在整个组织利益相关者层面传播信息技术（IT）安全的价值。 |
| T0026 | 编写和编写程序开发和后续修订的文档，在编码指令中插入注释，以便其他人可以理解程序。 |
| T0027 | 对日志文件，证据和其他信息进行分析，以确定识别网络入侵行为人的最佳方法。 |
| T0028 | 对企业网络资产进行和/或支持授权渗透测试。 |
| T0029 | 进行功能和连接测试以确保持续的可操作性。 |
| T0030 | 进行交互式培训练习，创造有效的学习环境。 |
| T0031 | 对被害人和证人进行面谈，并对嫌疑人进行面谈或盘问。 |
| T0032 | 为适当的安全控制执行应用程序安全设计的隐私影响评估（PIA），以保护个人身份信息（PII）的机密性和完整性。 |
| T0033 | 进行风险分析，可行性研究和/或权衡分析，以开发，记录和改进功能要求和规范。 |
| T0034 | 与系统分析师，工程师，程序员和其他人共同设计应用程序并获取有关项目限制和功能，性能要求和界面的信息。 |
| T0035 | 配置和优化网络集线器，路由器和交换机（例如，更高级别的协议，隧道）。 |
| T0036 | 如果可能，通过动态分析识别入侵后，确认已知的入侵事件并发现新信息。 |
| T0037 | 构建信息套件（例如链接页面）的访问路径以促进最终用户的访问。 |
| T0038 | 根据客户访谈和要求开发威胁模型。 |

| | |
|---|---|
| T0039 | 咨询客户以评估功能要求。 |
| T0040 | 咨询工程人员以评估硬件和软件之间的接口。 |
| T0041 | 协调并为企业级网络防御技术人员提供专家技术支持来解决网络防御事件。 |
| T0042 | 与网络防御分析师协调，管理和管理专业网络防御应用程序的规则和签名更新（例如入侵检测/防护系统，防病毒和内容黑名单）。 |
| T0043 | 与企业范围的网络防御人员协调以验证网络警报。 |
| T0044 | 与利益相关方合作，建立企业运营计划，战略和任务保证的连续性。 |
| T0045 | 根据需要与系统架构师和开发人员协调，以提供设计解决方案开发的监督。 |
| T0046 | 通过适当修改并重新检查程序来纠正错误，以确保产生期望的结果。 |
| T0047 | 将事件数据关联起来以确定具体的漏洞并提出可以迅速补救的建议。 |
| T0048 | 创建法证声明的证据副本（即法医图像），确保原始证据不被无意修改，以用于数据恢复和分析过程。这包括但不限于硬盘驱动器，软盘，CD，PDA，手机，GPS 和所有磁带格式。 |
| T0049 | 使用技术手段解密查获的数据。 |
| T0050 | 发生灾难性故障事件后，定义并区分重要系统功能或部分或全部系统恢复所需的业务功能的优先级。 |
| T0051 | 根据关键系统功能定义适当的系统可用性级别，并确保系统要求确定适当的灾难恢复和操作要求的连续性，以包括系统恢复/恢复的任何适当的故障切换/备用现场要求，备份要求和材料可支持性要求。 |
| T0052 | 根据客户要求定义项目范围和目标。 |
| T0053 | 设计和开发网络安全或支持网络安全的产品。 |
| T0054 | 设计组策略和访问控制列表，以确保与组织标准，业务规则和需求的兼容性。 |
| T0055 | 设计硬件，操作系统和软件应用程序以充分解决网络安全需求。 |
| T0056 | 将适当的数据备份功能设计或整合到整个系统设计中，并确保存在适当的技术和程序流程以实现安全的系统备份和受保护的备份数据存储。 |
| T0057 | 设计，开发和修改软件系统，使用科学分析和数学模型来预测和测量设计的结果和后果。 |
| T0058 | 根据测试结果确定开发能力的保证水平。 |
| T0059 | 制定计划，利用计算机和互联网调查涉嫌的犯罪，违规行为或可疑活动。 |

| | |
|---|---|
| T0060 | 了解信息最终用户的需求和要求。 |
| T0061 | 开发和指导系统测试和验证程序和文档。 |
| T0062 | 开发和记录设计过程和过程的要求，能力和约束条件。 |
| T0063 | 开发和记录系统管理标准操作程序。 |
| T0064 | 审查和验证数据挖掘和数据仓库程序，流程和要求。 |
| T0065 | 开发和实施网络备份和恢复程序。 |
| T0066 | 制定和维护战略计划。 |
| T0067 | 开发符合技术规范的体系结构或系统组件。 |
| T0068 | 制定数据标准，政策和程序。 |
| T0069 | 为组件和接口规范制定详细的安全设计文档，以支持系统设计和开发。 |
| T0070 | 制定正在开发的系统的灾难恢复和运营计划连续性，并确保在系统进入生产环境之前进行测试。 |
| T0071 | 为具有多级安全要求或要求的系统和网络开发/整合网络安全设计，以处理主要适用于政府组织（例如，UNCLASSIFIED，SECRET 和 TOP SECRET）的多个分类级别的数据。 |
| T0072 | 制定方法来监测和衡量风险，合规和保证工作。 |
| T0073 | 开发新的或确定适合目标受众的现有意识和培训材料。 |
| T0074 | 制定政策，计划和实施准则。 |
| T0075 | 按照既定的报告程序提供调查结果的技术总结。 |
| T0076 | 制定风险缓解策略来解决漏洞，并根据需要向系统或系统组件推荐安全更改。 |
| T0077 | 开发安全的代码和错误处理。 |
| T0078 | 针对系统和/或应用制定特定的网络安全对策和风险缓解策略。 |
| T0079 | 制定规范以确保风险，合规性和保证工作符合软件应用程序，系统和网络环境级别的安全性，弹性和可靠性要求。 |
| T0080 | 制定测试计划来解决规范和要求。 |
| T0081 | 诊断网络连接问题。 |
| T0082 | 在整个采购生命周期中记录和解决组织的信息安全，网络安全体系结构和系统安全工程要求。 |
| T0083 | 系统运行初步或剩余安全风险的草案。 |

| | |
|---|---|
| T0084 | 采用安全的配置管理流程。 |
| T0085 | 确保所有系统安全操作和维护活动都得到适当记录并根据需要进行更新。 |
| T0086 | 确保集成到系统设计中的商业产品安全补丁的应用满足管理机构针对预期操作环境所规定的时间表。 |
| T0087 | 确保按照联邦证据规则获得的所有数字媒体都遵循监管链。 |
| T0088 | 确保支持网络安全的产品或其他补偿安全控制技术将已识别的风险降低到可接受的水平。 |
| T0089 | 确保根据需要评估，验证和实施安全改进措施。 |
| T0090 | 确保获得或开发的系统和体系结构与组织的网络安全体系结构准则保持一致。 |
| T0091 | 确保网络安全检查，测试和审查与网络环境相协调。 |
| T0092 | 确保将网络安全要求纳入该系统和/或组织的连续性规划中。 |
| T0093 | 确保使用 IS 安全工程方法获取或开发保护和检测功能，并与组织级网络安全体系结构保持一致。 |
| T0094 | 与利益相关者建立和保持沟通渠道。 |
| T0095 | 利用组织的整体安全策略建立整体企业信息安全架构（EISA）。 |
| T0096 | 在事件响应团队与其他组织（例如法律部门）和外部（例如执法机构，供应商，公共关系专业人士）之间建立关系（如果适用）。 |
| T0097 | 评估和批准开发工作以确保基本安全防护措施得到适当安装。 |
| T0098 | 评估合同以确保符合资金，法律和计划要求。 |
| T0099 | 评估决策过程中的成本/收益，经济和风险分析。 |
| T0100 | 评估诸如所需报告格式，成本限制以及安全限制需求等因素以确定硬件配置。 |
| T0101 | 评估现有培训计划的有效性和全面性。 |
| T0102 | 评估法律，法规，政策，标准或程序的有效性。 |
| T0103 | 检查恢复的数据以获取与手头问题相关的信息。 |
| T0104 | 融合计算机网络攻击分析与犯罪和反间谍调查和操作。 |
| T0105 | 识别组件或元素，为这些元素分配安全功能，并描述元素之间的关系。 |
| T0106 | 确定替代信息安全策略以解决组织安全目标。 |
| T0107 | 识别并指导在测试和实施新系统期间遇到的技术问题的补救（例如，识别和寻找不可互操作的通信协议的解决方案）。 |

| | |
|---|---|
| T0108 | 与组织利益相关方合作确定关键业务职能并确定优先顺序。 |
| T0109 | 根据整体系统对连续性和可用性的要求，确定系统故障后或系统恢复事件期间支持基本功能或业务功能以恢复或恢复所需的基本系统功能或子系统的优先级。 |
| T0110 | 识别和/或确定安全事件是否指示违反需要采取特定法律行动的法律。 |
| T0111 | 高层次识别基本的常见编码缺陷。 |
| T0112 | 识别证据价值的数据或情报，以支持反间谍和刑事调查。 |
| T0113 | 以避免无意中改变的方式识别用于检查和分析的数字证据。 |
| T0114 | 确定犯罪证据要素。 |
| T0115 | 确定新技术或技术升级对信息技术（IT）安全计划的影响。 |
| T0116 | 确定组织政策利益相关者。 |
| T0117 | 在软件开发中确定整个企业计算机系统的集中和分散环境中的安全影响和应用方法。 |
| T0118 | 识别稳态运行和软件管理方面的安全问题，并纳入当产品达到使用寿命时必须采取的安全措施。 |
| T0119 | 识别，评估和推荐网络安全或支持网络安全的产品，以便在系统内使用，并确保推荐的产品符合组织的评估和验证要求。 |
| T0120 | 识别，收集和抓住文件或物理证据，包括与网络入侵事件，调查和操作相关的数字媒体和日志。 |
| T0121 | 实施新的系统设计程序，测试程序和质量标准。 |
| T0122 | 为新的或现有的系统实施安全设计。 |
| T0123 | 为系统和/或应用实施特定的网络安全对策。 |
| T0124 | 将网络安全漏洞解决方案纳入系统设计（例如，网络安全漏洞警报）。 |
| T0125 | 安装和维护网络基础设施设备操作系统软件（例如 IOS，固件）。 |
| T0126 | 安装或更换网络集线器，路由器和交换机。 |
| T0127 | 整合并整合信息安全和/或网络安全策略，以确保系统分析符合安全要求。 |
| T0128 | 集成自动化功能，用于在实际情况下更新或修补系统软件，并根据系统运行环境的当前和计划修补程序时间线要求，手动更新和修补系统软件的过程和程序。 |

| | |
|---|---|
| T0129 | 将新系统集成到现有网络体系结构中。 |
| T0130 | 与外部组织（例如，公共事务，执法部门，司令部或组件检查总长）的接口，以确保事件和其他计算机网络防御信息的适当和准确传播。 |
| T0131 | 解释和适用法律，法规，政策，标准或程序以解决具体问题。 |
| T0132 | 解释和/或批准有关新信息技术能力的安全要求。 |
| T0133 | 解释不合规的模式，以确定其对企业网络安全计划的风险水平和/或整体有效性的影响。 |
| T0134 | 领导并使信息技术（IT）安全优先事项与安全策略保持一致。 |
| T0135 | 领导和监督信息安全预算，人员配置和合同。 |
| T0136 | 根据组织策略维护基准系统安全性。 |
| T0137 | 维护数据库管理系统软件。 |
| T0138 | 维护可部署的网络防御审计工具包（例如专门的网络防御软件和硬件）以支持网络防御审计任务。 |
| T0139 | 维护目录复制服务，使信息能够通过优化路由从后端服务器自动复制到转发单元。 |
| T0140 | 通过发布，订阅和提醒功能维护信息交流，使用户能够根据需要发送和接收关键信息。 |
| T0141 | 维护信息系统保证和认证资料。 |
| T0142 | 保持与网络防御审计专门相关的适用网络防御政策，法规和合规性文件的相关知识。 |
| T0143 | 根据测试结果提出建议。 |
| T0144 | 管理帐户，网络权限以及访问系统和设备。 |
| T0145 | 管理和批准认证包（例如，ISO / IEC 15026-2）。 |
| T0146 | 管理数据的编译，编目，缓存，分发和检索。 |
| T0147 | 管理信息安全数据源的监控，以保持组织的情景意识。 |
| T0148 | 管理企业选区的计算机网络防御指南（例如，TCNO，运营概念，网络分析报告，NTSM，MTO）的发布。 |
| T0149 | 管理网络防御信息的威胁或目标分析，并在企业内部生成威胁信息。 |
| T0150 | 监视和评估系统对信息技术（IT）安全性，弹性和可靠性要求的遵从性。 |

| | |
|---|---|
| T0151 | 监控和评估企业网络安全保障措施的有效性，确保它们提供预期的保护级别。 |
| T0152 | 监控和维护数据库以确保最佳性能。 |
| T0153 | 监控网络容量和性能。 |
| T0154 | 监控并报告知识管理资产和资源的使用情况。 |
| T0155 | 记录并上报可能对环境造成持续和直接影响的事件（包括事件的历史，状态以及对进一步行动的潜在影响）。 |
| T0156 | 监督并提出有关配置管理的建议。 |
| T0157 | 监督信息安全培训和意识计划。 |
| T0158 | 在安全评估和授权过程中参与信息安全风险评估。 |
| T0159 | 参与制定或修改计算机环境网络安全计划的计划和要求。 |
| T0160 | 修补网络漏洞以确保信息得到外部方面的保护。 |
| T0161 | 执行来自各种来源（例如，单个主机日志，网络流量日志，防火墙日志和入侵检测系统[IDS]日志）的日志文件的分析以识别可能的网络安全威胁。 |
| T0162 | 执行数据库的备份和恢复以确保数据完整性。 |
| T0163 | 执行网络防御事件分类，包括确定范围，紧迫性和潜在影响，确定具体的漏洞，并提出可以迅速补救的建议。 |
| T0164 | 执行网络防御趋势分析和报告。 |
| T0165 | 执行动态分析以在本地环境中启动驱动器的“映像”（不必具有原始驱动器）以查看用户可能已经看到的入侵。 |
| T0166 | 使用从企业内各种来源收集的信息执行事件关联，以获得态势感知并确定观察到的攻击的有效性。 |
| T0167 | 执行文件签名分析。 |
| T0168 | 对建立的数据库执行哈希比较。 |
| T0169 | 对开发的应用程序和/或系统进行网络安全测试。 |
| T0170 | 执行初步的，法医学上可靠的图像收集，并检查以识别企业系统可能的缓解/修复。 |
| T0171 | 针对安全功能和弹性攻击执行集成质量保证测试。 |
| T0172 | 执行实时取证分析（例如，将 Helix 与 LiveView 结合使用）。 |
| T0173 | 执行时间线分析。 |

| | |
|---|---|
| T0174 | 执行需求分析以确定新的和改进的业务流程解决方案的机会。 |
| T0175 | 执行实时网络防御事件处理（例如法医收集，入侵关联和跟踪，威胁分析和直接系统修复）以支持可部署的事件响应小组（IRT）。 |
| T0176 | 执行安全编程并识别代码中的潜在缺陷以减轻漏洞。 |
| T0177 | 执行安全评估，找出安全架构中的差距，并制定安全风险管理计划。 |
| T0178 | 执行安全审查并确定安全体系结构中的安全漏洞，从而提出将其纳入风险缓解策略的建议。 |
| T0179 | 执行静态媒体分析。 |
| T0180 | 对专业网络防御应用程序和系统（例如防病毒，审计和修复）或虚拟专用网络（VPN）设备执行系统管理，以包括安装，配置，维护，备份和恢复。 |
| T0181 | 每当应用程序或系统发生重大变化时执行风险分析（例如，威胁，漏洞和发生概率）。 |
| T0182 | 执行第 1 层，第 2 层和第 3 层恶意软件分析。 |
| T0183 | 执行验证步骤，将实际结果与预期结果进行比较，并分析差异以确定影响和风险。 |
| T0184 | 为初始安装系统和网络规划和执行安全授权审查和保证案例开发。 |
| T0185 | 规划和管理知识管理项目的交付。 |
| T0186 | 规划，执行和验证数据冗余和系统恢复程序。 |
| T0187 | 根据锻炼结果或系统环境计划并建议修改或调整。 |
| T0188 | 准备识别技术和程序结果的审计报告，并提供建议的补救策略/解决方案。 |
| T0189 | 准备描述输入，输出和逻辑操作的详细工作流程图和图表，并将它们转换为用计算机语言编码的一系列指令。 |
| T0190 | 通过确保数据完整性（例如，根据标准操作程序编写阻止程序），准备用于成像的数字媒体。 |
| T0191 | 准备用例来证明对特定信息技术（IT）解决方案的需求。 |
| T0192 | 准备，分发和维护有关网络系统操作安全的计划，说明，指导和标准操作程序。 |
| T0193 | 处理犯罪现场。 |
| T0194 | 正确记录所有系统安全实施，操作和维护活动，并根据需要进行更新。 |

| | |
|---|---|
| T0195 | 根据任务要求提供管理的相关信息（通过网络门户或其他方式）。 |
| T0196 | 提供有关项目成本，设计概念或设计更改的建议。 |
| T0197 | 提供对软件应用程序，系统或网络的准确技术评估，记录相对于相关网络安全合规性的安全态势，功能和漏洞。 |
| T0198 | 提供与网络防御实践相关的网络事件和活动的每日总结报告。 |
| T0199 | 为运营计划持续性的发展提供企业网络安全和供应链风险管理指导。 |
| T0200 | 提供关于网络要求的反馈，包括网络架构和基础设施 |
| T0201 | 为客户或安装团队实施开发的系统提供指导。 |
| T0202 | 为领导提供网络安全指导。 |
| T0203 | 提供关于安保要求的意见，以列入工作说明和其他适当的采购文件。 |
| T0204 | 为实施计划和标准操作程序提供输入。 |
| T0205 | 为风险管理框架过程活动和相关文件（如系统生命周期支持计划，操作概念，操作程序和维护培训材料）提供输入。 |
| T0206 | 为信息技术（IT）人员提供领导和指导，确保向与他们职责相称的运营人员提供网络安全意识，基础知识，扫盲和培训。 |
| T0207 | 提供持续的优化和问题解决支持。 |
| T0208 | 为可能的改进和升级提供建议。 |
| T0209 | 就数据结构和数据库提供建议，确保报告/管理信息的正确和高质量的生产。 |
| T0210 | 提供有关新数据库技术和体系结构的建议。 |
| T0211 | 提供与网络安全要求有关的系统相关意见，以列入工作说明和其他适当的采购文件。 |
| T0212 | 就数字证据事宜向适当的人员提供技术援助。 |
| T0213 | 向上级总部提供技术文件，事故报告，计算机考试结果，总结和其他情境意识信息。 |
| T0214 | 接收并分析来自企业内各种来源的网络警报，并确定此类警报的可能原因。 |
| T0215 | 认识到可能存在的安全违规行为，并根据需要采取适当措施报告事件。 |
| T0216 | 识别并准确报告指示特定操作系统的法医文物。 |
| T0217 | 解决软件验收阶段的安全隐患，包括完成标准，风险接受和文件记录，通用标准和独立测试方法。 |

| | |
|---|---|
| T0218 | 根据评论结果推荐新的或修订的安全性，弹性和可靠性度量。 |
| T0219 | 推荐安全操作和维护组织的网络安全要求所需的资源分配。 |
| T0220 | 解决法律，法规，政策，标准或程序中的冲突。 |
| T0221 | 审核授权和保证文件，以确认每个软件应用程序，系统和网络的风险水平在可接受的范围内。 |
| T0222 | 与利益相关方一起审查现有和拟议的政 |
| T0223 | 审查或进行信息技术（IT）计划和项目的审计。 |
| T0224 | 查看培训文档（例如，课程内容文件[CCD]，课程计划，学生文本，考试，授课计划[SOI]和课程描述）。 |
| T0225 | 保护电子设备或信息源。 |
| T0226 | 为机构和跨部门政策委员会服务。 |
| T0227 | 推荐政策并协调审批。 |
| T0228 | 存储，检索和处理数据以分析系统功能和需求。 |
| T0229 | 在发现网络安全事件或漏洞时监督或管理保护措施或纠正措施。 |
| T0230 | 支持练习场景的设计和执行。 |
| T0231 | 为安全/认证测试和评估活动提供支持。 |
| T0232 | 测试和维护网络基础设施，包括软件和硬件设备。 |
| T0233 | 跟踪和记录从最初检测到最终解决方案的网络防御事件。 |
| T0234 | 跟踪审计结果和建议，确保采取适当的缓解行动。 |
| T0235 | 将功能需求转换为技术解决方案 |
| T0236 | 将安全需求转换为应用程序设计元素，包括记录软件攻击面的元素，执行威胁建模以及定义任何特定的安全标准。 |
| T0237 | 排除系统硬件和软件故障。 |
| T0238 | 使用数据雕刻技术（例如，Forensic Tool Kit [FTK]，Foremost）提取数据。 |
| T0239 | 使用联邦和组织特定的已发布文档来管理其计算环境系统的操作。 |
| T0240 | 使用网络监视工具捕获和分析与恶意活动相关的网络流量。 |
| T0241 | 使用专门的设备和技术来编目，记录，提取，收集，打包和保存数字证据。 |
| T0242 | 利用模型和模拟来分析或预测不同操作条件下的系统性能。 |
| T0243 | 验证并更新反映应用程序/系统安全设计功能的安全文档。 |

| | |
|---|---|
| T0244 | 验证应用程序软件/网络/系统安全状态是按照说明实施的，文档偏差，并建议采取必要的措施来纠正这些偏差。 |
| T0245 | 确认软件应用程序/网络/系统认证和保证文档是最新的。 |
| T0246 | 撰写并发布网络防御技术，指导和事件发现报告给合适的选区。 |
| T0247 | 编写指导性材料（例如标准操作程序，生产手册），为相关部分的劳动力提供详细指导。 |
| T0248 | 提高管理层对安全问题的认识，并确保良好的安全原则反映在组织的愿景和目标中。 |
| T0249 | 研究当前技术来了解所需系统或网络的功能。 |
| T0250 | 根据任务要求确定定制硬件和软件开发的网络功能策略。 |
| T0251 | 为外部服务（例如，云服务提供商，数据中心）开发安全合规流程和/或审计。 |
| T0252 | 在适当的环境下进行必要的评审（例如技术监督，对策评论[TSCM]，TEMPEST对策评审）。 |
| T0253 | 进行粗略的二进制分析。 |
| T0254 | 监督政策标准和实施策略，确保程序和指导方针符合网络安全政策。 |
| T0255 | 参与风险管理流程，以提供安全风险，缓解措施和对其他技术风险的意见。 |
| T0256 | 通过采购活动评估采购职能在解决信息安全要求和供应链风险方面的有效性并提出改进建议。 |
| T0257 | 确定范围，基础设施，资源和数据样本大小，以确保系统要求得到充分证明。 |
| T0258 | 提供可能的攻击/入侵，异常活动和误用活动的及时检测，识别和告警，并将这些事件和事件与良性活动区分开来。 |
| T0259 | 使用网络防御工具对系统活动进行持续监控和分析，以识别恶意活动。 |
| T0260 | 分析确定的恶意活动以确定利用漏洞，利用方法，对系统和信息的影响。 |
| T0261 | 协助确定关键的网络防御基础设施和关键资源，确定优先次序并协调保护。 |
| T0262 | 采用经过批准的纵深防御原则和实践（例如，防御复合地点，分层防御，安全稳健性）。 |
| T0263 | 在系统生命周期的所有阶段确定特定于信息技术（IT）系统的安全需求。 |
| T0264 | 确保针对风险评估，审计，检查等过程中发现的漏洞采取行动计划，里程碑计划或补救计划。 |

| | |
|---|---|
| T0265 | 确保安全要求和适当的信息技术（IT）政策和程序的成功实施和功能符合组织的使命和目标。 |
| T0266 | 按照新的或更新的应用程序的要求执行渗透测试。 |
| T0267 | 针对潜在的利用编程语言弱点和系统和元素中的漏洞设计对策和缓解措施。 |
| T0268 | 定义并记录新系统或系统间新接口的实现如何影响当前环境的安全状态。 |
| T0269 | 设计和开发关键管理职能（与网络安全相关）。 |
| T0270 | 分析用户需求和要求，以规划和执行系统安全性开发。 |
| T0271 | 开发网络安全设计以满足特定的运营需求和环境因素（例如访问控制，自动化应用，联网操作，高完整性和可用性要求，多级安全/多级分级处理以及处理敏感分区信息）。 |
| T0272 | 确保安全设计和网络安全开发活动得到适当记录（提供安全实施的功能描述）并根据需要进行更新。 |
| T0273 | 酌情制定并记录关键系统要素的供应链风险。 |
| T0274 | 创建安全措施的可审计证据。 |
| T0275 | 支持必要的合规活动（例如，确保遵循系统安全配置准则，发生合规性监控）。 |
| T0276 | 按照适当的供应链风险管理惯例，根据需要参与收购流程。 |
| T0277 | 确保所有收购，采购和外包工作满足符合组织目标的信息安全要求。 |
| T0278 | 收集入侵伪像（例如，源代码，恶意软件，特洛伊木马）并使用发现的数据来缓解企业内潜在的网络防御事件。 |
| T0279 | 担任执法人员的技术专家和联络员，并根据需要解释事件详情。 |
| T0280 | 根据政策/指导方针/程序/法规/法律持续验证组织，以确保合规。 |
| T0281 | 预测持续的服务需求，并确保安全假设在必要时进行评估。 |
| T0282 | 定义和/或实施政策和程序，以确保适当保护关键基础设施。 |
| T0283 | 与利益相关方合作识别和/或开发适当的解决方案技术。 |
| T0284 | 设计和开发与网络安全相关的新工具/技术。 |
| T0285 | 在数字媒体上执行病毒扫描。 |
| T0286 | 执行文件系统取证分析。 |
| T0287 | 执行静态分析以安装驱动器的“映像”（不必具有原始驱动器）。 |

| | |
|---|---|
| T0288 | 执行静态恶意软件分析。 |
| T0289 | 根据需要使用可部署的取证工具包来支持操作。 |
| T0290 | 确定入侵集的策略，技术和程序（TTP）。 |
| T0291 | 检查网络拓扑结构以了解通过网络的数据流。 |
| T0292 | 推荐计算环境漏洞更正。 |
| T0293 | 使用元数据识别和分析网络流量中的异常情况。 |
| T0294 | 在各种各样的源数据集（指示和警告）中进行研究，分析和关联。 |
| T0295 | 使用数据包分析工具验证入侵检测系统（IDS）针对网络流量的警报。 |
| T0296 | 隔离并删除恶意软件。 |
| T0297 | 基于网络流量识别网络设备的应用程序和操作系统。 |
| T0298 | 根据网络流量重建恶意攻击或活动。 |
| T0299 | 识别网络映射和操作系统（OS）指纹识别活动。 |
| T0300 | 开发和记录用户体验（UX）要求，包括信息体系结构和用户界面要求。 |
| T0301 | 为应用软件/网络/系统开发和实施独立于网络安全的审计流程，并监督正在进行的独立审计，以确保运营和研究与设计（R&D）流程和程序符合组织和强制性网络安全要求，系统管理员和其他网络安全人员在进行日常活动时。 |
| T0302 | 开发合同语言以确保符合供应链，系统，网络和运营安全。 |
| T0303 | 在设计和开发安全应用程序时识别并利用企业级版本控制系统。 |
| T0304 | 将系统开发生命周期（SDLC）方法（如 IBM Rational Unified Process）实施并集成到开发环境中。 |
| T0305 | 为数据库和数据管理系统执行配置管理，问题管理，容量管理和财务管理。 |
| T0306 | 支持数据库和数据管理系统的事件管理，服务级别管理，变更管理，发布管理，连续性管理和可用性管理。 |
| T0307 | 分析候选架构，分配安全服务并选择安全机制。 |
| T0308 | 分析新兴趋势的事件数据。 |
| T0309 | 评估安全控制的有效性。 |
| T0310 | 协助构建可在网络防御网络工具上实施的签名，以响应网络环境或飞地内的新威胁或观察到的威胁。 |
| T0311 | 咨询客户有关软件系统设计和维护的信息。 |

| | |
|---|---|
| T0312 | 与情报分析师协调关联威胁评估数据。 |
| T0313 | 设计和记录质量标准。 |
| T0314 | 开发系统安全环境，初步系统安全操作概念（CONOPS），并根据适用的网络安全要求定义基准系统安全要求。 |
| T0315 | 开发并提供技术培训以教育他人或满足客户需求。 |
| T0316 | 开发或协助开发基于计算机的培训模块或课程。 |
| T0317 | 制定或协助制定课程作业。 |
| T0318 | 开发或协助开发课程评估。 |
| T0319 | 制定或协助制定评分和熟练水平标准。 |
| T0320 | 协助制定个人/集体发展，培训和/或补救计划。 |
| T0321 | 制定或协助制定学习目标和目标。 |
| T0322 | 制定或协助制定在职培训材料或计划。 |
| T0323 | 开发或协助开发用于衡量和评估学习者熟练程度的书面测试。 |
| T0324 | 直接软件编程和文档开发。 |
| T0325 | 记录系统的目的和初步的系统安全操作概念。 |
| T0326 | 采用配置管理流程。 |
| T0327 | 评估网络基础设施漏洞以增强正在开发的功能。 |
| T0328 | 评估安全体系结构和设计，以确定提供或提供的安全设计和体系结构是否足以满足采购文档中的要求。 |
| T0329 | 遵循软件和系统工程生命周期标准和流程。 |
| T0330 | 保持有保证的信息传递系统。 |
| T0331 | 维护事件跟踪和解决方案数据库。 |
| T0332 | 根据组织的网络事件响应计划，通知指定的管理人员，网络事故响应人员和网络安全服务提供商团队成员发生可疑的网络事件，并明确事件的历史，状态和对进一步行动的潜在影响。 |
| T0334 | 确保所有系统组件都可以集成和对齐（例如，过程，数据库，策略，软件和硬件）。 |
| T0335 | 构建，安装，配置和测试专用的网络防御硬件。 |
| T0336 | 撤回：与 T0228 集成 |

| | |
|---|---|
| T0337 | 监督和指派工作给程序员，设计师，技术人员和技术人员，以及其他工程和科学人员。 |
| T0338 | 编写详细的功能规范，记录架构开发过程。 |
| T0339 | 领导努力促进该组织利用知识管理和信息共享。 |
| T0340 | 充当支持服务的基础信息技术（IT）运营流程和功能的主要利益相关者，提供指导和监控所有重要活动，以便成功交付服务。 |
| T0341 | 倡导为网络培训资源提供充足的资金，包括内部和行业提供的课程，教师和相关材料。 |
| T0342 | 分析数据来源以提供可操作的建议。 |
| T0343 | 分析危机以确保公共，个人和资源保护。 |
| T0344 | 评估所有配置管理（更改配置/发布管理）流程。 |
| T0345 | 根据教学技术使用和学生学习，知识转移和满意度的轻松程度，评估教学的有效性和效率。 |
| T0346 | 评估个人受害人，证人或嫌疑人与调查有关的行为。 |
| T0347 | 评估源数据和后续结果的有效性。 |
| T0348 | 协助评估实施和维护专用网络防御基础设施的影响。 |
| T0349 | 收集指标和趋势数据。 |
| T0350 | 开展市场分析，以确定，评估和推荐商用，政府现货和开源产品，以便在系统内使用，并确保推荐的产品符合组织的评估和验证要求。 |
| T0351 | 使用统计过程进行假设检验。 |
| T0352 | 进行学习需求评估并确定需求。 |
| T0353 | 与系统分析师，工程师，程序员和其他人共同设计应用程序。 |
| T0354 | 协调和管理为客户端到端提供的整体服务。 |
| T0355 | 与内部和外部主题专家协调，以确保现有资格标准反映组织功能要求并符合行业标准。 |
| T0356 | 与组织人力资源利益相关者协调，确保适当分配和分配人力资本资产。 |
| T0357 | 创建交互式学习练习以创建有效的学习环境。 |
| T0358 | 为特权访问用户设计和开发系统管理和管理功能。 |

| | |
|---|---|
| T0359 | 设计，实施，测试和评估信息系统，物理系统和/或嵌入式技术之间的安全接口。 |
| T0360 | 确定威胁的程度并建议采取行动或对策来减轻风险。 |
| T0361 | 开发和促进数据收集方法。 |
| T0362 | 根据既定的网络工作角色制定和实施标准化职位描述。 |
| T0363 | 根据现行人力资源政策制定并审查招聘，雇用和保留程序。 |
| T0364 | 发展网络职业领域分类结构，包括建立职业领域的入门要求和其他术语，如代码和标识符。 |
| T0365 | 制定或协助制定网络培训培训政策和协议。 |
| T0366 | 从大数据集开发战略洞察力。 |
| T0367 | 制定网络课程的目标和目标。 |
| T0368 | 确保网络职业领域按照组织人力资源政策和指示进行管理。 |
| T0369 | 确保网络劳动力管理政策和流程符合关于机会均等，多样性和公平招聘/雇佣惯例的法律和组织要求。 |
| T0370 | 确保已经定义了适当的服务水平协议（SLA）和基础合同，明确规定了客户对服务的描述和监控服务的措施。 |
| T0371 | 为软件应用程序，网络或系统建立可接受的限制。 |
| T0372 | 建立并收集指标以监控和验证网络员工就绪情况，包括分析网络员工数据，以评估已确定，填补并由合格人员填补的职位状态。 |
| T0373 | 建立并监督网络职业领域入学和培训资格要求的豁免程序。 |
| T0374 | 建立网络职业道路，让职业发展，有意识的发展，以及网络职业领域内和之间的发展。 |
| T0375 | 建立人力，人员和资质数据元素标准以支持网络员工队伍管理和报告要求。 |
| T0376 | 根据组织要求建立，资源，实施和评估网络员工队伍管理计划。 |
| T0377 | 收集有关客户满意度和内部服务绩效的反馈信息，以促进持续改进。 |
| T0378 | 整合风险驱动的系统维护更新过程，以解决系统缺陷（定期和不按周期）。 |
| T0379 | 管理与支持服务的信息技术（IT）流程所有者之间的内部关系，协助定义和达成运营级别协议（OLA）。 |

| | |
|---|---|
| T0380 | 与教育工作者和培训师一起制定教学策略，例如讲座，演示，互动练习，多媒体演示，视频课程，网络课程以获得最有效的学习环境。 |
| T0381 | 向技术和非技术受众提供技术信息。 |
| T0382 | 以创意形式呈现数据。 |
| T0383 | 编程自定义算法。 |
| T0384 | 提高管理层对网络政策和战略的认识，并确保组织的使命，愿景和目标体现出合理的原则。 |
| T0385 | 根据数据分析和调查结果向关键利益相关者提供可行的建议。 |
| T0386 | 在司法过程中向审判律师提供刑事调查支持。 |
| T0387 | 审查并应用网络职业领域资格标准。 |
| T0388 | 审查和应用有关或影响网络员工队伍的组织政策。 |
| T0389 | 审查服务绩效报告，确定任何重大问题和差异，在必要时启动纠正措施并确保所有未决问题得到跟进。 |
| T0390 | 审查/评估网络员工队伍的有效性，以调整技能和/或资格标准。 |
| T0391 | 支持将合格的网络员工人员整合到信息系统生命周期开发流程中。 |
| T0392 | 利用技术文档或资源实施新的数学，数据科学或计算机科学方法。 |
| T0393 | 验证可测试性的规范和要求。 |
| T0394 | 与其他服务经理和产品所有者合作来平衡服务并优先考虑服务，以满足客户的总体要求，限制和目标。 |
| T0395 | 在行动评论后撰写并发布。 |
| T0396 | 根据分析师的目标使用适当的工具处理图像。 |
| T0397 | 执行 Windows 注册表分析。 |
| T0398 | 通过动态分析识别入侵后，对正在运行的系统执行文件和注册表监视。 |
| T0399 | 将媒体信息输入到已获取的数字媒体的跟踪数据库（例如，产品跟踪工具）中。 |
| T0400 | 关联事件数据并执行网络防御报告。 |
| T0401 | 维护可部署的网络防御工具包（例如专门的网络防御软件/硬件）以支持事件响应小组的任务。 |
| T0402 | 在数据管理系统的设计中有效分配存储容量。 |

| | |
|---|---|
| T0403 | 在 Windows 和 UNIX 系统上（例如执行诸如以下任务的任务的读取，解释，编写，修改和执行简单脚本（例如 Perl，VBScript）：解析大型数据文件，自动执行手动任务以及获取/处理远程数据） 。 |
| T0404 | 利用不同的编程语言编写代码，打开文件，读取文件并将输出写入不同的文件。 |
| T0405 | 使用 R 等开源语言并应用定量技术（例如描述性和推理性统计，抽样，实验设计，差异的参数和非参数测试，普通最小二乘回归，一般线）。 |
| T0406 | 确保设计和开发活动得到适当记录（提供实施的功能描述）并根据需要进行更新。 |
| T0407 | 必要时参与收购流程。 |
| T0408 | 解释和适用适用的法律，法规和监管文件并融入政策。 |
| T0409 | 在整个产品设计，开发和预启动阶段对原型设计和流程问题进行故障排除。 |
| T0410 | 确定功能和安全相关的功能，以寻找新功能开发的机会，以利用或减轻漏洞。 |
| T0411 | 识别和/或开发反向工程工具以增强功能并检测漏洞。 |
| T0412 | 为获取系统和软件进行导入/导出评估。 |
| T0413 | 开发数据管理功能（例如，基于云的集中式加密密钥管理），以支持移动员工队伍。 |
| T0414 | 开发供应链，系统，网络，性能和网络安全要求。 |
| T0415 | 确保供应链，系统，网络，性能和网络安全要求包含在合同语言中并交付。 |
| T0416 | 通过利用现有的公共密钥基础设施（PKI）库并在适当时合并证书管理和加密功能，启用具有公共密钥的应用程序。 |
| T0417 | 在适当的时候设计和开发安全应用程序（例如企业 PKI，联合身份识别服务器，企业防病毒解决方案）时，识别并利用企业范围的安全服务。 |
| T0418 | 安装，更新和排除系统/服务器的故障。 |
| T0419 | 获取和维护有关法律，法规，政策，协议，标准，程序或其他通告中出现的宪法问题的工作知识。 |
| T0420 | 管理测试平台，测试和评估服务提供商管理的应用程序，硬件基础结构，规则/签名，访问控制和平台配置。 |

| | |
|---|---|
| T0421 | 管理显式组织知识的索引/编目，存储和访问（例如，硬拷贝文档，数字文件）。 |
| T0422 | 实施数据管理标准，要求和规范。 |
| T0423 | 分析反恐情报或犯罪活动的计算机生成的威胁。 |
| T0424 | 分析并向利益相关者提供信息，以支持安全应用程序的开发或现有安全应用程序的修改。 |
| T0425 | 分析组织网络政策。 |
| T0426 | 分析软件，硬件或互操作性测试的结果。 |
| T0427 | 分析用户需求和要求以规划架构。 |
| T0428 | 分析安全需求和软件需求，以确定在时间和成本限制以及安全要求下的设计可行性。 |
| T0429 | 评估政策需求并与利益相关方合作制定管理网络活动的政策。 |
| T0430 | 收集并保存用于起诉计算机犯罪的证据。 |
| T0431 | 检查系统硬件的可用性，功能，完整性和效率。 |
| T0432 | 收集并分析入侵工件（例如，源代码，恶意软件和系统配置）并使用发现的数据来缓解企业内潜在的网络防御事件。 |
| T0433 | 对日志文件，证据和其他信息进行分析，以确定识别网络入侵或其他犯罪行为人的最佳方法。 |
| T0434 | 进行诉状框架，以正确识别违反法律，法规或政策/指导的指控。 |
| T0435 | 定期进行系统维护，包括清理（物理和电子），磁盘检查，例行重启，数据转储和测试。 |
| T0436 | 对程序和软件应用程序进行试运行，以确保生成期望的信息并且指令和安全级别正确。 |
| T0437 | 将培训和学习与商业或任务要求相关联。 |
| T0438 | 在专门的网络防御系统（例如，防火墙和入侵防御系统）上创建，编辑和管理网络访问控制列表。 |
| T0439 | 检测和分析加密数据，速记，备用数据流和其他形式的隐藏数据。 |
| T0440 | 在灾难性故障事件发生后，捕获并整合部分或全部系统恢复所需的基本系统功能或业务功能。 |

| | |
|---|---|
| T0441 | 定义并整合当前和未来的任务环境。 |
| T0442 | 创建针对观众和物理环境的培训课程。 |
| T0443 | 提供适合观众和物理/虚拟环境的培训课程。 |
| T0444 | 将概念，程序，软件，设备和/或技术应用程序应用于学生。 |
| T0445 | 设计/整合网络战略，概述与组织战略计划相一致的愿景，使命和目标。 |
| T0446 | 设计，开发，集成和更新提供机密性，完整性，可用性，身份验证和不可否认性的系统安全措施。 |
| T0447 | 设计硬件，操作系统和软件应用程序以充分满足需求。 |
| T0448 | 开发满足用户需求所需的企业体系结构或系统组件。 |
| T0449 | 根据安全要求进行设计，以确保满足所有系统和/或应用的要求。 |
| T0450 | 根据需求设计培训课程和课程内容。 |
| T0451 | 参与培训课程和课程内容的开发。 |
| T0452 | 设计，构建，实施和维护知识管理框架，为最终用户提供对组织智力资本的访问。 |
| T0453 | 确定和发展潜在客户并确定信息来源以识别和/或起诉肇事者或其他犯罪行为的责任方。 |
| T0454 | 根据适用的准则定义基准安全要求。 |
| T0455 | 开发软件系统测试和验证程序，编程和文档。 |
| T0456 | 开发安全的软件测试和验证程序。 |
| T0457 | 开发系统测试和验证程序，编程和文档。 |
| T0458 | 遵守组织系统管理标准操作程序。 |
| T0459 | 实施数据挖掘和数据仓库应用程序。 |
| T0460 | 开发和实施数据挖掘和数据仓库程序。 |
| T0461 | 实施和执行本地网络使用政策和程序。 |
| T0462 | 根据系统可用性要求，制定程序并测试系统操作故障转移到备用站点。 |
| T0463 | 为新的或修改的系统开发成本估算。 |
| T0464 | 为组件和接口规范制定详细的设计文档，以支持系统设计和开发。 |
| T0465 | 制定实施准则。 |
| T0466 | 开发缓解策略来解决成本，进度，性能和安全风险。 |

| | |
|---|---|
| T0467 | 确保培训符合网络安全培训，教育或意识的目标和目标。 |
| T0468 | 诊断并解决客户报告的系统事件，问题和事件。 |
| T0469 | 分析和报告组织安全态势趋势。 |
| T0470 | 分析和报告系统安全态势趋势。 |
| T0471 | 记录数字和/或相关证据的原始状况（例如，通过数码照片，书面报告，散列函数检查）。 |
| T0472 | 草案，工作人员和发布网络政策。 |
| T0473 | 根据需要记录和更新所有定义和架构活动。 |
| T0474 | 向监察长，隐私官员，监督和合规人员提供有关遵守网络安全政策和相关法律法规要求的法律分析和决策。 |
| T0475 | 根据最小特权和需要知道的原则评估适当的访问控制。 |
| T0476 | 评估法律，法规，政策，标准或程序变更的影响。 |
| T0477 | 确保执行灾难恢复和操作的连续性。 |
| T0478 | 向管理层，人员或客户提供有关法律，法规，政策，标准或程序的指导。 |
| T0479 | 利用信息技术（IT）系统和数字存储媒体解决，调查和/或起诉针对人员和财产的网络犯罪和欺诈行为。 |
| T0480 | 识别组件或元素，分配全面的功能组件以包含安全功能，并描述元素之间的关系。 |
| T0481 | 确定并解决网络员工队伍规划和管理问题（例如招聘，保留和培训）。 |
| T0482 | 根据趋势分析提出建议，改进软件和硬件解决方案，以提高客户体验。 |
| T0483 | 识别与实施任何网络防御工具（例如，工具和签名测试和优化）的潜在冲突。 |
| T0484 | 确定信息系统和网络以及文件的保护需求（即安全控制）。 |
| T0485 | 实施安全措施来解决漏洞，降低风险，并根据需要向系统或系统组件推荐安全更改。 |
| T0486 | 对企业内的专用网络防御系统实施风险管理框架（RMF）/安全评估和授权（SA＆A）要求，并为其记录和保存记录。 |
| T0487 | 促进执行新的或修订的法律，法规，行政命令，政策，标准或程序。 |
| T0488 | 实施新的或现有系统的设计。 |

| | |
|---|---|
| T0489 | 按照既定程序实施系统安全措施，以确保机密性，完整性，可用性，身份验证和不可否认性。 |
| T0490 | 安装和配置数据库管理系统和软件。 |
| T0491 | 按照组织标准为系统用户安装和配置硬件，软件和外围设备。 |
| T0492 | 确保在安全的环境中集成和实施跨域解决方案（CDS）。 |
| T0493 | 领导和监督预算，人员配置和合同。 |
| T0494 | 管理帐户，网络权限和对系统和设备的访问。 |
| T0495 | 管理认证包（例如，ISO / IEC 15026-2）。 |
| T0496 | 执行资产管理/库存信息技术（IT）资源。 |
| T0497 | 管理信息技术（IT）规划流程，以确保开发的解决方案能够满足客户的要求。 |
| T0498 | 管理系统/服务器资源，包括性能，容量，可用性，适用性和可恢复性。 |
| T0499 | 减轻/纠正安全/认证测试期间发现的安全缺陷和/或建议适当的高级领导或授权代表接受风险。 |
| T0500 | 修改和维护现有软件以纠正错误，使其适应新的硬件，或升级接口并提高性能。 |
| T0501 | 监视和维护系统/服务器配置。 |
| T0502 | 监视和报告客户端计算机系统性能。 |
| T0503 | 监视外部数据源（例如，网络防御供应商站点，计算机紧急响应小组，安全焦点）以维护网络防御威胁状态的货币并确定哪些安全问题可能对企业产生影响。 |
| T0504 | 评估和监测与系统实施和测试实践相关的网络安全。 |
| T0505 | 监控网络政策，原则和实践在提供规划和管理服务方面的严格应用。 |
| T0506 | 就利益相关者提出的政策变更达成共识。 |
| T0507 | 监督系统组件的安装，实施，配置和支持。 |
| T0508 | 验证所有应用程序的最低安全要求。 |
| T0509 | 执行信息安全风险评估。 |
| T0510 | 协调事件响应功能。 |
| T0511 | 对开发中的系统进行开发测试。 |
| T0512 | 对与其他系统交换电子信息的系统进行互操作性测试。 |

| | |
|---|---|
| T0513 | 执行操作测试。 |
| T0514 | 诊断有问题的系统/服务器硬件。 |
| T0515 | 在出现故障的系统/服务器硬件上执行修复。 |
| T0516 | 执行安全的程序测试，审查和/或评估以识别代码中的潜在缺陷并减轻漏洞。 |
| T0517 | 整合有关识别安全架构差距的结果。 |
| T0518 | 执行安全审查并确定架构中的安全漏洞。 |
| T0519 | 为最有效的学习环境规划和协调教室技术和格式（例如讲座，演示，互动练习，多媒体演示）的交付。 |
| T0520 | 规划非课堂教学技术和格式（例如，视频课程，指导，网络课程）。 |
| T0521 | 规划实施策略以确保企业组件可以整合和对齐。 |
| T0522 | 准备法律文件和其他相关文件（例如，陈述，简介，宣誓书，声明，上诉，书状，发现）。 |
| T0523 | 按照法律标准和要求准备报告以记录调查情况。 |
| T0524 | 通过组织的运营流程和系统促进信息所有者/用户之间的知识共享。 |
| T0525 | 提供企业网络安全和供应链风险管理指导。 |
| T0526 | 根据重大威胁和漏洞向领导层提供网络安全建议。 |
| T0527 | 为与信息系统安全相关的实施计划和标准操作程序提供输入。 |
| T0528 | 为实施计划，标准操作程序，维护文档和维护培训材料提供输入 |
| T0529 | 为网络管理人员和用户提供政策指导。 |
| T0530 | 开发趋势分析和影响报告。 |
| T0531 | 解决硬件/软件接口和互操作性问题。 |
| T0532 | 审查取证图像和其他数据源（例如易失性数据）以恢复潜在的相关信息。 |
| T0533 | 审查，开展或参与网络计划和项目的审计。 |
| T0534 | 对准确性，完整性和货币（例如，课程内容文件，课程计划，学生文本，考试，教学时间表和课程描述）进行定期评估/修订课程内容。 |
| T0535 | 根据以往培训课程的反馈，推荐对课程和课程内容进行修订。 |
| T0536 | 担任自己专业领域（如技术，版权，印刷媒体，电子媒体）的内部顾问和顾问。 |
| T0537 | 支持 CIO 制定网络相关政策。 |

| | |
|---|---|
| T0538 | 为测试和评估活动提供支持。 |
| T0539 | 测试，评估和验证硬件和/或软件，以确定是否符合规定的规范和要求。 |
| T0540 | 记录和管理测试数据。 |
| T0541 | 跟踪系统要求来设计组件并执行差距分析。 |
| T0542 | 将建议的功能转换为技术要求。 |
| T0544 | 验证系统架构的稳定性，互操作性，可移植性和/或可伸缩性。 |
| T0545 | 与利益相关方合作解决计算机安全事件和漏洞合规性。 |
| T0546 | 撰写并发布网络辩护建议，报告和关于事件调查结果的白皮书给合适的选区。 |
| T0547 | 研究和评估可用的技术和标准以满足客户的要求。 |
| T0548 | 为灾难恢复，应急和运营计划的连续性提供建议和意见。 |
| T0549 | 对相关技术重点领域（例如本地计算环境，网络和基础设施，飞地边界，支持基础设施和应用）进行技术（技术评估）和非技术（评估人员和运营）风险和漏洞评估。 |
| T0550 | 就选择具有成本效益的安全控制措施以降低风险（如保护信息，系统和流程）提出建议。 |
| T0551 | 起草和发布供应链安全和风险管理文件。 |
| T0552 | 审核并批准供应链安全/风险管理政策。 |
| T0553 | 应用网络安全功能（例如加密，访问控制和身份管理）以减少开发机会。 |
| T0554 | 确定并记录软件补丁或软件易受攻击的版本范围。 |
| T0555 | 记录系统之间新系统或新界面的实施如何影响当前和目标环境，包括但不限于安全状态。 |
| T0556 | 评估和设计与网络空间相关的安全管理功能。 |
| T0557 | 整合与网络空间相关的密钥管理功能。 |
| T0558 | 分析用户需求和要求，规划和开展系统开发。 |
| T0559 | 开发设计以满足特定的运营需求和环境因素（例如访问控制，自动化应用，联网操作。 |
| T0560 | 协作网络安全设计以满足特定的运营需求和环境因素（例如，访问控制，自动化应用，联网操作，高完整性和可用性要求，多级安全/多级分级处理以及处理敏感分区信息）。 |

| | |
|---|---|
| T0561 | 准确表征目标。 |
| T0562 | 调整收集操作或收集计划以解决已确定的问题/挑战，并将收集与整体操作要求同步。 |
| T0563 | 为分析，设计，开发或获取用于实现目标的功能提供输入。 |
| T0564 | 分析反馈以确定收集产品和服务满足要求的程度。 |
| T0565 | 分析传入的收集请求。 |
| T0566 | 分析内部操作体系结构，工具和程序，以提高性能。 |
| T0567 | 分析目标操作体系结构以获取访问权限。 |
| T0568 | 分析影响馆藏管理运作结构和要求（例如持续时间，范围，沟通要求，机构间/国际协议）的因素的计划，指示，指导和政策。 |
| T0569 | 回答请求信息。 |
| T0570 | 应用和利用授权的网络功能来访问目标网络。 |
| T0571 | 应用政策和流程的专业知识，促进计划和/或协议备忘录的发展，谈判和内部人员配置。 |
| T0572 | 应用网络收集，环境准备和参与专业知识，以实现新的开发和/或持续收集操作，或支持客户的要求。 |
| T0573 | 评估并将营运环境因素和风险应用于收集管理流程。 |
| T0574 | 适用并遵守适用的法律，法律，法规和政策。 |
| T0575 | 为业务计划活动协调情报支持。 |
| T0576 | 评估所有来源的情报并建议支持网络运营目标的目标。 |
| T0577 | 评估现有信息交换和管理系统的效率。 |
| T0578 | 根据规定的规格评估收集资产的绩效。 |
| T0579 | 评估目标漏洞和/或操作能力以确定行动方针。 |
| T0580 | 评估馆藏在满足优先信息差距，使用现有能力和方法方面的有效性，并相应调整收集策略和收集要求。 |
| T0581 | 协助并建议机构间合作伙伴确定和制定最佳实践，以促进实现组织目标的业务支持。 |
| T0582 | 为行动发展提供专业知识。 |
| T0583 | 提供主题专业知识以制定共同的业务图景。 |

| | |
|---|---|
| T0584 | 保持一个共同的情报图片。 |
| T0585 | 提供主题专业知识以开发网络操作特定指标。 |
| T0586 | 协助协调，验证和管理全源采集要求，计划和/或活动。 |
| T0587 | 协助制定和完善优先信息要求。 |
| T0588 | 提供专业知识来制定措施的有效性和措施。 |
| T0589 | 协助确定情报收集不足。 |
| T0590 | 根据需要启用跨合作伙伴组织的智能支持计划的同步。 |
| T0591 | 对目标基础设施开发活动进行分析。 |
| T0592 | 提供识别网络相关成功标准的信息。 |
| T0593 | 简要威胁和/或目标当前情况。 |
| T0594 | 建立和维护电子目标文件夹。 |
| T0595 | 按照分类准则分类文件。 |
| T0596 | 一旦满足关闭信息请求。 |
| T0597 | 与涉及相关领域的情报分析员/定位组织合作。 |
| T0598 | 与开发组织协作创建和部署实现目标所需的工具。 |
| T0599 | 与涉及相关网络领域的其他客户，情报和定位组织进行协作。 |
| T0600 | 与其他内部和外部合作伙伴组织就目标访问和操作问题进行协作。 |
| T0601 | 与其他团队成员或合作组织合作开发各种信息材料（例如网页，简报，印刷材料）。 |
| T0602 | 与客户协作定义信息需求。 |
| T0603 | 向领导层，内部和外部客户传达新的发展，突破，挑战和经验教训。 |
| T0604 | 将分配和可用资产与通过需求表示的收款需求进行比较。 |
| T0605 | 汇编收集管理活动执行组织收集目标的经验教训。 |
| T0606 | 针对特定目标编译，整合和/或解释所有来源的数据以获得智能或漏洞价值。 |
| T0607 | 识别并对目标通信进行分析以确定支持操作所必需的信息。 |
| T0608 | 对物理和逻辑数字技术（如无线，SCADA，电信）进行分析以确定可能的接入途径。 |
| T0609 | 进行无线计算机和数字网络的访问。 |
| T0610 | 进行无线计算机和数字网络的收集和处理。 |

| | |
|---|---|
| T0611 | 进行作业结束评估。 |
| T0612 | 开展无线计算机和数字网络的开发。 |
| T0613 | 按照既定的指导方针和程序对收集要求进行正式和非正式的协调。 |
| T0614 | 进行独立深入的目标和技术分析，包括导致访问的目标特定信息（例如文化，组织，政治）。 |
| T0615 | 进行深入的研究和分析。 |
| T0616 | 对网络内的系统进行网络侦察和漏洞分析。 |
| T0617 | 进行节点分析。 |
| T0618 | 开展网上活动以控制和渗透部署技术的数据。 |
| T0619 | 开展网上和网外活动以控制和渗透部署的自动化技术的数据。 |
| T0620 | 通过各种在线工具进行开源数据收集。 |
| T0621 | 进行质量控制，以确定收集到的关于网络的信息的有效性和相关性。 |
| T0622 | 制定，审查和实施支持网络运营的各级规划指导。 |
| T0623 | 对计算机和数字网络进行调查。 |
| T0624 | 进行目标研究和分析。 |
| T0625 | 考虑收集资产和资源的效率和有效性，如果/应用于优先信息要求。 |
| T0626 | 使用既定的指导和程序构建收集计划和矩阵。 |
| T0627 | 为网络行动的危机行动规划做出贡献。 |
| T0628 | 必要时为组织的决策支持工具的发展做出贡献。 |
| T0629 | 与适当的内部和/或外部决策者一起致力于网络运营政策，绩效标准，计划和批准包的开发，人员配置和协调。 |
| T0630 | 将情报股份纳入网络作战计划的总体设计中。 |
| T0631 | 根据优先收集要求和收集纪律引导协调收集资产的资源分配。 |
| T0632 | 协调将收集计划纳入适当的文件。 |
| T0633 | 与适当的合作伙伴协调目标审查。 |
| T0634 | 重新执行或重新引导收集资产和资源。 |
| T0635 | 与情报和网络防御合作伙伴协调获取相关的重要信息。 |
| T0636 | 与情报规划人员协调，确保收集管理人员收到信息要求。 |
| T0637 | 与情报规划小组协调，评估满足指定情报任务的能力。 |

| | |
|---|---|
| T0638 | 协调，制作和跟踪情报需求。 |
| T0639 | 协调，同步和起草网络作战计划的适用情报部分。 |
| T0640 | 利用情报估计来对付潜在的目标行动。 |
| T0641 | 创建识别可利用的技术或操作漏洞的综合开发策略。 |
| T0642 | 保持对内部和外部网络组织结构，优势以及员工和技术的使用的意识。 |
| T0643 | 将工具部署到目标并在部署后使用它们（例如，后门，嗅探器）。 |
| T0644 | 检测针对目标网络和主机的漏洞利用情况并做出相应反应。 |
| T0645 | 确定解决目标，指导和运营环境变化的行动方针。 |
| T0646 | 确定现有的收集管理网页数据库，图书馆和仓库。 |
| T0647 | 确定识别因素如何影响任务，收集，处理，利用和传播架构的形式和功能。 |
| T0648 | 确定最适合具体网络运营目标的指标（如有效性度量）。 |
| T0649 | 确定具有所有可访问收集资产收集权限的组织和/或梯队。 |
| T0650 | 确定给定目标使用的技术。 |
| T0651 | 开发一种比较收集报告和突出要求的方法来识别信息差距。 |
| T0652 | 开发全源情报定位材料。 |
| T0653 | 应用分析技术获取更多目标信息。 |
| T0654 | 制定和维持有意和/或危机计划。 |
| T0655 | 制定并审查具体的网络行动指导，以便融入更广泛的规划活动。 |
| T0656 | 制定和审查情报指导，以整合到支持网络作战计划和执行。 |
| T0657 | 根据收集纪律制定操作每个阶段的协调指示。 |
| T0658 | 制定网络运营计划和指导，确保执行和资源分配决策与组织目标保持一致。 |
| T0659 | 为网络运营要求提供详细的情报支持。 |
| T0660 | 制定回答优先信息请求所需的信息要求。 |
| T0661 | 制定措施的有效性和措施。 |
| T0662 | 根据领导层的指导，优先事项和/或业务重点分配收集资产。 |
| T0663 | 开发必须的有效性评估或作战评估材料。 |
| T0664 | 开发获取和保持访问目标系统的新技术。 |
| T0665 | 制定或参与制定提供，请求和/或获得外部合作伙伴支持以同步网络运营的标准。 |

| | |
|---|---|
| T0666 | 制定或制定国际网络参与战略，政策和活动以实现组织目标。 |
| T0667 | 制定潜在的行动方案。 |
| T0668 | 制定向收集经理，资产经理，加工，开发和传播中心提供反馈的程序。 |
| T0669 | 为合作伙伴计划，运营和能力开发制定战略和流程。 |
| T0670 | 制定，实施并建议对适当的计划程序和政策进行更改。 |
| T0671 | 与外部合作伙伴开发，维护和评估网络合作安全协议。 |
| T0672 | 设计，记录和验证网络运营策略和规划文档。 |
| T0673 | 传播报告，通知决策者收集问题。 |
| T0674 | 传播任务信息和收集计划。 |
| T0675 | 使用既定程序对收集结果进行评估并记录。 |
| T0676 | 网络情报收集和生产要求草案。 |
| T0677 | 编辑或执行 Windows 和 UNIX 系统上的简单脚本（例如 Perl，VBScript）。 |
| T0678 | 吸引客户了解客户的情报需求。 |
| T0679 | 确保运营计划工作有效地转换到当前运营。 |
| T0680 | 确保情报规划活动与业务规划时间表相结合并保持同步。 |
| T0681 | 建立替代性加工，开发和传播途径以解决已确定的问题或问题。 |
| T0682 | 验证收集请求和关键信息要求与领导层的优先情报要求之间的关系。 |
| T0683 | 使用批准的指导和/或程序建立加工，开发和传播管理活动。 |
| T0684 | 估计通过网络活动产生的操作效果。 |
| T0685 | 评估威胁决策过程。 |
| T0686 | 识别威胁漏洞。 |
| T0687 | 识别对 Blue Force 漏洞的威胁。 |
| T0688 | 根据预期效果评估可用功能，以推荐有效的解决方案。 |
| T0689 | 评估收集到的信息和/或产生的情报满足信息请求的程度。 |
| T0690 | 评估情报评估以支持规划周期。 |
| T0691 | 评估影响可用网络情报能力就业的条件。 |
| T0692 | 生成并评估网络分析策略的有效性。 |
| T0693 | 评估收集操作与操作要求同步的程度。 |
| T0694 | 根据收集计划评估收集操作的有效性。 |

| | |
|---|---|
| T0695 | 检查拦截相关的元数据和内容，了解定位的重要性。 |
| T0696 | 利用各种方法或工具利用网络设备，安全设备和/或终端或环境。 |
| T0697 | 通过物理和/或无线手段促进访问。 |
| T0698 | 与图片管理者共同进行可视化输入以提供持续更新的情报和监视。 |
| T0699 | 促进内部和外部合作伙伴决策者之间的互动，以同步和整合支持目标的行动方案。 |
| T0700 | 促进整个网络作业界共享“最佳做法”和“经验教训”。 |
| T0701 | 与开发人员协作，在提交工具要求中传达目标和技术知识，以加强工具开发。 |
| T0702 | 根据现有情报学科能力的知识制定收集策略，并收集使多学科收集能力和访问与目标及其可观察性相一致的方法。 |
| T0703 | 收集并分析数据（例如有效性度量）以确定有效性，并为后续活动提供报告。 |
| T0704 | 将网络运营和通信安全支持计划纳入组织目标。 |
| T0705 | 结合情报和反情报来支持计划的制定。 |
| T0706 | 通过传统和替代技术收集有关网络的信息（例如，社交网络分析，呼叫链接，流量分析）。 |
| T0707 | 生成信息请求。 |
| T0708 | 确定威胁策略和方法。 |
| T0709 | 确定支持网络操作的所有可用的合作伙伴智能功能和限制。 |
| T0710 | 识别和评估威胁关键功能，需求和漏洞。 |
| T0711 | 识别，起草，评估相关情报或信息要求并对其进行优先排序。 |
| T0712 | 与外部合作伙伴确定并管理安全合作重点。 |
| T0713 | 确定并提交智能要求，用于指定优先信息要求。 |
| T0714 | 确定协作论坛，这些协作论坛可以作为与指定组织和职能团体协调流程，职能和产出的机制。 |
| T0715 | 根据目标确定收集差距和潜在收集策略。 |
| T0716 | 与指定的收集当局确定协调要求和程序。 |
| T0717 | 确定关键的目标元素。 |
| T0718 | 识别情报差距和不足。 |
| T0719 | 识别网络运营规划中的网络情报差距和不足。 |

| | |
|---|---|
| T0720 | 找出我们对目标技术理解的差距并开发创新的收集方法。 |
| T0721 | 确定可能干扰和/或降低处理，利用和传播架构效率的问题或问题。 |
| T0722 | 确定网络组件及其功能以实现分析和目标开发。 |
| T0723 | 根据优先级信息要求识别潜在的应用程序收集规则。 |
| T0724 | 识别网络中潜在的力量和脆弱点。 |
| T0725 | 确定并减少集合管理能力的风险，以支持计划，运营和目标周期。 |
| T0726 | 确定适用的情报环境准备派生产品的需求，范围和时间表。 |
| T0727 | 通过地理空间分析技术识别，定位和跟踪目标。 |
| T0728 | 根据威胁因素提供投入或制定行动方案。 |
| T0729 | 通知外部合作伙伴新的或修订的关于网络运营合作活动的政策和指导的潜在影响。 |
| T0730 | 使用既定程序向利益相关者（例如收集管理者，资产管理者，加工，利用和传播中心）通报评估结果。 |
| T0731 | 发起请求来指导任务并协助收集管理。 |
| T0732 | 将网络计划/定位工作与其他组织进行整合。 |
| T0733 | 解释环境准备评估以确定行动过程。 |
| T0734 | 发布信息请求。 |
| T0735 | 领导和协调对作战计划的情报支持。 |
| T0736 | 领导或启用开采操作以支持组织目标和目标需求。 |
| T0737 | 将优先收集要求与优化资产和资源相关联。 |
| T0738 | 保持对硬件和软件技术进步的认识（例如参加培训或会议，阅读）及其潜在影响。 |
| T0739 | 与参与网络规划或相关领域的内部和外部合作伙伴保持关系。 |
| T0740 | 保持有机运营基础设施的情景意识和功能。 |
| T0741 | 保持与网络相关的情报需求和相关任务的态势感知。 |
| T0742 | 保持合作伙伴能力和活动的情景意识。 |
| T0743 | 保持态势感知，以确定操作环境的变化是否需要审查计划。 |
| T0744 | 维护目标列表（即 RTL，JTL，CTL 等）。 |
| T0745 | 建议指导收集以支持客户要求。 |

| | |
|---|---|
| T0746 | 根据需要修改收集要求。 |
| T0747 | 监控和评估综合网络运营，以确定实现组织目标的机会。 |
| T0748 | 监视并报告与指定的网络操作警告问题集有关的威胁处置，活动，策略，能力，目标等方面的变化。 |
| T0749 | 监视并报告已验证的威胁活动。 |
| T0750 | 监测重新分配收集工作的完成情况。 |
| T0751 | 监视开放源代码网站是否存在针对组织或合作伙伴兴趣的恶意内容。 |
| T0752 | 监督运营环境并报告满足领导优先信息要求的对抗活动。 |
| T0753 | 监测处理，利用和传播架构的运行状态和有效性。 |
| T0754 | 监视目标网络，以提供目标通信更改或处理失败的指示和警告。 |
| T0755 | 监控运营环境，以了解收集运营管理流程的潜在因素和风险。 |
| T0756 | 操作和维护用于获取和维护对目标系统的访问的自动化系统。 |
| T0757 | 优化收集资产和资源的组合，以提高与优先情报要求相关的重要信息的有效性和效率。 |
| T0758 | 制作及时的融合式全源网络操作智能和/或适应症和警告智能产品（例如威胁评估，情况介绍，情报研究，国家研究）。 |
| T0759 | 有助于审查和完善政策，包括评估批准或不批准此类政策的后果。 |
| T0760 | 根据需要向主管团队，协调小组和专责小组提供主题专业知识。 |
| T0761 | 酌情为计划/发展论坛和工作组提供主题方面的专业知识和支持。 |
| T0763 | 与网络活动的内部和外部合作伙伴进行长期的战略规划工作。 |
| T0764 | 提供主题专业知识，与内部和外部网络运营合作伙伴一起规划工作。 |
| T0765 | 提供主题专业知识来开发练习。 |
| T0766 | 提出管理与外部协调小组互动的政策。 |
| T0767 | 执行内容和/或元数据分析以满足组织目标。 |
| T0768 | 开展网络活动以降低/消除计算机和计算机网络中的信息。 |
| T0769 | 执行定位自动化活动。 |
| T0770 | 网站特征。 |
| T0771 | 将主题专业知识提供给网站特征描述。 |
| T0772 | 为练习做好准备并提供主题专业知识。 |

| | |
|---|---|
| T0773 | 基于平台功能优先收集平台的收集要求。 |
| T0774 | 处理泄露的数据以便分析和/或传播给客户。 |
| T0775 | 生成网络重建。 |
| T0776 | 制作目标系统分析产品。 |
| T0777 | 配置文件网络或系统管理员及其活动。 |
| T0778 | 配置文件目标及其活动。 |
| T0779 | 为运营和情报决策者提供建议/协助，根据动态的运营情况重新分配收集资产和资源。 |
| T0780 | 提供咨询和倡导支持，促进收集规划，作为战略运动计划和其他适应性计划的一个组成部分。 |
| T0781 | 提供瞄准点和再接触建议。 |
| T0782 | 为有效性评估提供分析和支持。 |
| T0783 | 酌情为关键的内部/外部利益相关者提供当前的情报支持。 |
| T0784 | 提供针对智能支持计划输入的针对网络的指导和建议。 |
| T0785 | 提供必要的评估和反馈，以提高情报生产，情报报告，采集要求和作业。 |
| T0786 | 提供信息和评估以便通知领导层和客户;发展和完善目标;支持运营计划和执行;并评估操作的效果。 |
| T0787 | 为制定和完善网络运营目标，优先事项，战略，计划和计划提供投入。 |
| T0788 | 提供意见并协助行动后有效性评估。 |
| T0789 | 提供意见并协助制定计划和指导。 |
| T0790 | 为领导接受度的目标效果评估提供输入。 |
| T0791 | 为运营支持计划的行政和后勤部分提供投入。 |
| T0792 | 为指定的练习，计划活动和时间敏感操作提供情报分析和支持。 |
| T0793 | 为指定的练习和/或时间敏感的操作提供有效性支持。 |
| T0794 | 提供操作和重新接入建议。 |
| T0795 | 为内部和外部合作伙伴提供计划支持。 |
| T0796 | 提供实时可操作的地理位置信息。 |
| T0797 | 提供符合领导目标的目标建议。 |
| T0798 | 按指定提供定位产品和定位支持。 |

| | |
|---|---|
| T0799 | 提供时间敏感的定位支持。 |
| T0800 | 及时通知可能影响组织目标，资源或能力的迫切意图或敌对意图或活动。 |
| T0801 | 建议适当时改进，适应，终止和执行操作计划。 |
| T0802 | 审查适当的信息来源以确定所收集信息的有效性和相关性。 |
| T0803 | 以图表或报告格式重建网络。 |
| T0804 | 在旨在实现网络效应的行动中，针对目标记录信息收集和/或环境准备活动。 |
| T0805 | 报告情报衍生的重大网络事件和入侵。 |
| T0806 | 根据批准的指导和/或程序要求使用纪律处理，开发和传播使用纪律收集资产和资源收集的信息。 |
| T0807 | 研究新兴技术（计算机和电话网络，卫星，有线和无线）在开放和分类资源中的通信趋势。 |
| T0808 | 审查和理解组织领导目标和计划指导。 |
| T0809 | 审查分配的收集资产的功能。 |
| T0810 | 审查情报收集指导的准确性/适用性。 |
| T0811 | 审查优先收集要求和重要信息清单。 |
| T0812 | 根据需要审查和更新总体收集计划。 |
| T0813 | 审查，批准，优先考虑并提交研究，开发和/或获取网络能力的运营要求。 |
| T0814 | 根据最佳资产和资源的可用性修改收集矩阵。 |
| T0815 | 消毒和减少信息以保护来源和方法。 |
| T0816 | 网络智能规划工作的范围。 |
| T0817 | 通过识别可协助调查复杂或异常情况的主题专家，作为合作伙伴团队信息的渠道。 |
| T0818 | 作为与外部合作伙伴的联络人。 |
| T0819 | 征求和管理完成对请求者的反馈，以反映收集要求的收集质量，及时性和有效性。 |
| T0820 | 指定需要对收集资产和资源进行重新分配或重新定向的收集计划和/或操作环境的更改。 |
| T0821 | 指定必须在近期内执行的特定于纪律的集合和/或任务。 |
| T0822 | 将信息请求提交给收集需求管理部分以作为收集请求进行处理。 |

| | |
|---|---|
| T0823 | 提交或回复请求解除网络操作冲突。 |
| T0824 | 支持识别和记录附带效应。 |
| T0825 | 酌情同步网络国际参与活动和相关资源需求。 |
| T0826 | 同步安全合作计划的网络部分。 |
| T0827 | 使用可用的协作功能和技术同步所有可用的有机和合作伙伴情报收集资产的综合就业。 |
| T0828 | 测试和评估本地开发的可用于操作的工具。 |
| T0829 | 针对目标工具测试内部开发的工具和技术。 |
| T0830 | 跟踪信息请求的状态，包括那些使用已建立的程序作为收集请求和生产要求处理的请求。 |
| T0831 | 将收集请求转换为适用的特定学科收集要求。 |
| T0832 | 使用反馈结果（例如，吸取的教训）来识别提高收集管理效率和有效性的机会。 |
| T0833 | 根据既定标准验证信息请求。 |
| T0834 | 与规划人员，情报分析人员和收集经理密切合作，确保情报需求和收集计划的准确性和最新性。 |
| T0835 | 与计划人员，分析师和集合管理人员密切合作，确定情报差距并确保情报需求准确并且是最新的。 |
| T0836 | 记录传达事件和/或练习结果的经验教训。 |
| T0837 | 向管理人员和操作人员提供影响组织目标的语言和文化问题的建议。 |
| T0838 | 使用语言和/或文化专业知识分析和处理信息。 |
| T0839 | 评估，记录和应用目标的动机和/或参考框架，以促进分析，定位和收集机会。 |
| T0840 | 通过内部和/或外部组织方面的合作来加强收集，分析和传播。 |
| T0841 | 开展全源目标研究，包括在目标语言中使用开源资料。 |
| T0842 | 对目标通信进行分析以确定支持组织目标的重要信息。 |
| T0843 | 进行质量评审并提供关于转录或翻译材料的反馈。 |
| T0844 | 评估和解释元数据以查找模式，异常或事件，从而优化目标定位，分析和处理。 |
| T0845 | 确定网络威胁的策略和方法。 |

| | |
|---|---|
| T0846 | 确定全球网络内的目标通信。 |
| T0847 | 保持目标通信工具，技术和目标通信网络的特性（例如容量，功能，路径，关键节点）的意识及其对定位，收集和分析的潜在影响。 |
| T0848 | 向收集经理提供反馈，以加强未来的收集和分析。 |
| T0849 | 在初始源数据中进行外语和方言识别。 |
| T0850 | 执行或支持技术网络分析和映射。 |
| T0851 | 提供需求和反馈，以优化语言处理工具的开发。 |
| T0852 | 酌情进行社交网络分析和文档。 |
| T0853 | 扫描，识别目标图形（包括机器对机器通信）和/或语音语言材料并确定其优先级。 |
| T0854 | 向适当的客户提供关键或时间敏感的信息。 |
| T0855 | 用目标语言录制目标语音资料。 |
| T0856 | 翻译（例如，逐字，主旨和/或摘要）目标图形材料。 |
| T0857 | 翻译（例如，逐字，主旨和/或摘要）目标语音材料。 |
| T0858 | 识别计算机程序中的外语术语（例如注释，变量名称）。 |
| T0859 | 提供接近实时的语言分析支持（例如，实时操作）。 |
| T0860 | 用目标语言识别与网络/技术相关的术语。 |
| T0861 | 与总法律顾问，外部事务和企业合作，确保现有服务和新服务符合隐私和数据安全义务。 |
| T0862 | 与法律顾问和管理层，主要部门和委员会合作，确保组织拥有和保持适当的隐私和保密同意，授权表格和信息通告以及反映当前组织和法律实践和要求的材料。 |
| T0863 | 与适当的监管机构协调，确保涉及公民权利，公民自由和隐私考虑的方案，政策和程序以综合全面的方式处理。 |
| T0864 | 与监管和认证机构联络。 |
| T0865 | 与外部事务合作，发展与负责隐私和数据安全问题的监管机构和其他政府官员的关系。 |
| T0866 | 掌握适用的联邦和州的隐私法律和认证标准的现有知识，并监控信息隐私技术的进步，以确保组织的适应性和合规性。 |

| | |
|---|---|
| T0867 | 确保所有处理和/或数据库在需要时向当地隐私/数据保护机构进行注册。 |
| T0868 | 与业务团队和高级管理人员合作，确保意识到隐私和数据安全问题的“最佳实践”。 |
| T0869 | 与组织高级管理层合作，建立一个全组织的隐私监督委员会 |
| T0870 | 担任隐私监督委员会活动的领导角色 |
| T0871 | 协作处理网络隐私和安全政策和程序 |
| T0872 | 与网络安全人员就安全风险评估流程进行合作，以解决隐私合规性和风险缓解问题 |
| T0873 | 与高级管理层沟通，制定战略计划，以最大化价值的方式收集，使用和共享信息，同时遵守适用的隐私法规 |
| T0874 | 为企业官员提供有关信息资源和技术的战略指导 |
| T0875 | 协助安全官员开发和实施信息基础设施 |
| T0876 | 与公司合规官员协调记录和报告任何隐私侵犯证据的自我披露程序。 |
| T0877 | 与相关组织单位合作，负责监督消费者信息访问权 |
| T0878 | 作为技术系统用户的信息隐私联络员 |
| T0879 | 担任信息系统部门的联络员 |
| T0880 | 开发隐私培训材料和其他通信，以提高员工对公司隐私政策，数据处理实践和程序以及法律义务的理解 |
| T0881 | 监督，指导，交付或确保向所有员工，志愿者，承包商，联盟，商业伙伴和其他适当的第三方提供初始隐私培训和指导 |
| T0882 | 开展持续的隐私培训和提高认识活动 |
| T0883 | 与外部事务合作，与隐私和数据安全问题相关的消费者组织和其他非政府组织建立关系，并管理公司参与与隐私和数据安全相关的公共活动 |
| T0884 | 与组织管理部门，法律顾问和其他相关方合作，与包括承诺采纳或修改隐私立法，法规或标准的政府机构在内的外部各方代表组织的信息隐私利益。 |
| T0885 | 定期向董事会，首席执行官或其他负责人或委员会报告隐私计划的状况 |
| T0886 | 与外部事务部门合作，回应有关消费者和员工关注的有关数据的新闻和其他调查 |
| T0887 | 为组织的隐私计划提供领导 |

| | |
|---|---|
| T0888 | 指导和监督隐私专家，并与全球高级管理人员协调隐私和数据安全计划，以确保整个组织的一致性 |
| T0889 | 确保遵守隐私惯例并对未遵守组织工作人员中所有个人的隐私政策，扩大员工队伍以及与人力资源，信息安全官员，行政管理和法律顾问合作的所有业务伙伴遵守适用的隐私政策 |
| T0890 | 针对未遵守公司隐私政策和程序的情况制定适当的制裁措施 |
| T0891 | 解决不遵守公司隐私政策或信息实践通知的指控 |
| T0892 | 开发和协调隐私风险管理和合规框架 |
| T0893 | 对公司的数据和隐私项目进行全面审查，并确保它们符合企业隐私和数据安全目标和政策。 |
| T0894 | 开发和管理企业范围的程序，以确保新产品和服务的开发符合公司隐私政策和法律义务 |
| T0895 | 建立接收，记录，跟踪，调查和采取有关组织隐私政策和程序的所有投诉的流程 |
| T0896 | 与管理层和运营机构一起建立一个机制，在机构范围内并根据法律的要求跟踪受保护的健康信息的访问情况，并允许合格的个人审核或接收有关此类活动的报告 |
| T0897 | 提供隐私和安全相关项目的规划，设计和评估领导力 |
| T0898 | 建立内部隐私审计计划 |
| T0899 | 考虑到法律，监管或公司政策的变化，定期修改隐私计划 |
| T0900 | 提供发展指导，并协同组织管理和行政以及法律顾问协助确定，实施和维护组织信息隐私政策和程序 |
| T0901 | 确保技术的使用维护并且不侵蚀个人信息的使用，收集和披露方面的隐私保护 |
| T0902 | 监控系统开发和运营以确保安全和隐私合规性 |
| T0903 | 对建议的个人信息隐私规定进行隐私影响评估，包括收集的个人信息类型和受影响的人数 |
| T0904 | 定期进行信息隐私影响评估和持续的合规监督活动，与组织的其他合规和业务评估职能相协调 |
| T0905 | 审查所有系统相关的信息安全计划，以确保安全和隐私实践之间的一致性 |

| | |
|---|---|
| T0906 | 与所有涉及受保护信息发布方面的组织人员合作，确保与组织的政策，程序和法律要求的协调 |
| T0907 | 记录并管理个人和/或受保护信息的发布或披露请求 |
| T0908 | 制定和管理供应商审核和审核程序，以遵守隐私和数据安全政策和法律要求 |
| T0909 | 参与所有贸易伙伴和业务伙伴协议的实施和持续合规性监控，以确保解决所有隐私问题，要求和责任 |
| T0910 | 作为或与合作伙伴关系的律师一起工作 |
| T0911 | 减轻员工或业务合作伙伴使用或披露个人信息的影响 |
| T0912 | 制定并应用纠正措施程序 |
| T0913 | 对与本组织隐私政策和程序有关的所有投诉采取行动，必要时与法律顾问与其他类似职能进行协调和合作 |
| T0914 | 支持该组织的隐私合规计划，与隐私官，首席信息安全官和其他业务领导密切合作，确保遵守联邦和州的隐私法律和法规 |
| T0915 | 找出并纠正潜在的公司合规缺陷和/或风险领域，以确保完全符合隐私法规 |
| T0916 | 与隐私官，首席信息安全官，法律顾问和业务单位一起管理隐私事件和违规行为 |
| T0917 | 与首席信息安全官协调，确保安全和隐私惯例相一致 |
| T0918 | 建立，实施和维护全组织范围的政策和程序，以遵守隐私条例 |
| T0919 | 确保公司保留适当的隐私和保密声明，同意书和授权表格以及材料 |
| T0920 | 开发和维护适当的沟通和培训，以促进和教育所有员工和董事会成员关于隐私合规问题和要求以及不合规的后果 |
| T0921 | 确定与组织隐私计划相关的业务合作伙伴要求。 |
| T0922 | 建立并管理接收，记录，跟踪，调查和采取纠正措施的流程，以适当处理有关公司隐私政策和程序的投诉。 |
| T0923 | 在有关监管机构和其他法律实体以及组织官员的合规审查或调查中与其合作。 |
| T0924 | 执行持续的隐私合规监控活动。 |
| T0925 | 监控信息隐私技术的进步，确保组织的采用和合规性。 |
| T0926 | 开发或协助开发隐私培训材料和其他通信，以提高员工对公司隐私政策，数据处理实践和程序以及法律义务的理解。 |

| | |
|---|---|
| T0927 | 任命和指导 IT 安全专家团队。 |
| T0928 | 与主要利益相关方合作建立网络安全风险管理计划。 |
| T0929 | 识别并将个人分配到与执行风险管理框架相关的特定角色。 |
| T0930 | 为组织制定风险管理策略，包括确定风险容忍度。 |
| T0931 | 确定系统将支持的任务，业务功能和任务/业务流程。 |
| T0932 | 识别对系统的开发，实施，运行或维持有安全兴趣的利益相关者。 |
| T0933 | 识别对系统的开发，实施，运行或维持有安全兴趣的利益相关者。 |
| T0934 | 确定需要保护的利益相关者资产。 |
| T0935 | 对利益相关者资产进行初始风险评估并持续更新风险评估。 |
| T0936 | 定义利益相关者保护需求和利益相关者安全需求。 |
| T0937 | 确定系统在企业架构中的位置。 |
| T0938 | 确定可供组织系统继承系统范围的通用控制。 |
| T0939 | 对具有相同影响级别的组织系统进行二级安全分类。 |
| T0940 | 确定系统的边界。 |
| T0941 | 确定分配给系统和组织的安全要求。 |
| T0942 | 确定系统要处理，存储或传输的信息类型。 |
| T0943 | 对系统进行分类并将安全分类结果归档为系统要求的一部分。 |
| T0944 | 描述系统的特征。 |
| T0945 | 将系统注册到适当的组织计划/管理办公室。 |
| T0946 | 选择系统的安全控制并在安全计划中记录计划的控制实施的功能描述。 |
| T0947 | 制定监控安全控制有效性的战略;将系统级策略与组织和任务/业务流程级监控策略协调一致。 |
| T0948 | 审查并批准安全计划。 |
| T0949 | 实施安全计划或其他系统文档中指定的安全控制。 |
| T0950 | 记录对计划安全控制实施的更改并为系统建立配置基线。 |
| T0951 | 开发，审查和批准一个计划，以评估系统和组织中的安全控制。 |
| T0952 | 按照安全评估计划中规定的评估程序评估安全控制。 |
| T0953 | 准备一份安全评估报告，记录安全控制评估中发现的问题并提供建议。 |

| | |
|---|---|
| T0954 | 根据安全评估报告的调查结果和建议，对安全控制进行初步补救行动;重新评估补救措施。 |
| T0955 | 根据安全评估报告的调查结果和建议制定行动计划和里程碑，但不包括采取的任何补救措施。 |
| T0956 | 组装授权包，并将该包提交给授权官员进行裁决。 |
| T0957 | 确定操作或使用系统或提供或使用通用控制的风险。 |
| T0958 | 针对所确定的风险确定并实施一个首选的行动方案。 |
| T0959 | 确定系统操作或使用的风险，或提供或使用共同控制措施的风险是否可以接受。 |
| T0960 | 监视系统及其操作环境的变化。 |
| T0961 | 根据组织定义的监控策略评估系统内使用并继承的安全控制。 |
| T0962 | 根据正在进行的监测活动的结果，风险评估以及行动计划和里程碑中的未解决项目对风险做出响应。 |
| T0963 | 根据持续监测过程的结果更新安全计划，安全评估报告，行动计划和里程碑。 |
| T0964 | 根据监控策略持续向授权官员报告系统的安全状态（包括安全控制的有效性）。 |
| T0965 | 持续检查系统的安全状态（包括安全控制的有效性），以确定风险是否仍然可以接受。 |
| T0966 | 实施系统处理策略，在系统从服务中移除时执行所需的操作。 |
| T0967 | 赞助并促进组织内的持续监督。 |
| T0968 | 根据需要将工作人员分配给合适的持续监测工作组。 |
| T0969 | 确定报告要求以支持持续监测活动。 |
| T0970 | 建立评分和评分指标来衡量持续监测计划的有效性。 |
| T0971 | 确定如何将持续监控计划整合到组织的更广泛的信息安全治理结构和政策中。 |
| T0972 | 使用持续监控评分和评分指标来制定信息安全投资决策，以解决持续性问题。 |
| T0973 | 确保连续监测人员获得执行指定职责所需的培训和资源（如人员和预算）。 |
| T0974 | 与组织风险分析师合作，确保持续监控报告涵盖组织的适当级别。 |
| T0975 | 与组织风险分析师一起工作，确保风险度量标准能够真实定义以支持持续监控。 |

| | |
|---|---|
| T0976 | 与组织官员一起工作，确保持续监控工具数据提供风险意识。 |
| T0977 | 为持续监控数据建立不可接受的风险阈值触发器。 |
| T0978 | 与组织官员合作建立可供组织连续监测计划使用的系统级报告类别。 |
| T0980 | 指定一名合格人员负责连续监测计划的管理和实施。 |
| T0981 | 确定持续监控利益相关者并建立一个流程，让他们了解该计划。 |
| T0982 | 确定持续监控计划所实现的以安全为导向的组织报告要求。 |
| T0983 | 使用持续监控数据来制定信息安全投资决策以解决持续性问题。 |
| T0984 | 定义连续监控程序中的触发器，可用于定义不可接受的风险并导致采取措施解决。 |
| T0985 | 建立评分和评分指标来衡量持续监测计划的有效性。 |
| T0986 | 与安全管理人员合作，在系统级别建立适当的持续监控报告要求。 |
| T0987 | 使用持续监控工具和技术持续评估风险。 |
| T0988 | 根据连续监测计划中确定的标准建立适当的报告要求，以用于自动化控制评估。 |
| T0989 | 如果连续监测工具和技术的数据还不够充分或质量不足，则采用非自动化评估方法。 |
| T0990 | 与外部审计小组就如何分享持续监测计划的信息及其对安全控制评估的影响开发流程。 |
| T0991 | 确定用于自动化控制评估的报告要求，以支持持续监控。 |
| T0992 | 确定连续监测结果将如何用于持续授权。 |
| T0993 | 建立连续的监控工具和访问控制技术流程和程序。 |
| T0994 | 确保持续监控工具和技术访问控制得到充分管理。 |
| T0995 | 建立一个流程，为持续监控缓解措施提供技术帮助。 |
| T0996 | 协调不同用户的持续监控报告要求。 |
| T0997 | 建立支持每个连续监测工具或技术实施的责任。 |
| T0998 | 与评分和指标工作组建立联系以支持持续监测。 |
| T0999 | 建立并运行一个流程来管理引入新风险以支持持续监控。 |
| T1000 | 建立连续监测配置设置问题和协调子组。 |
| T1001 | 建立连续的监测工具和技术性能测量/管理要求。 |

| | |
|---|---|
| T1002 | 使用分数和等级来激励和评估绩效，同时解决问题以支持持续监控 |
| T1003 | 与安全管理人员（即系统所有者，信息系统安全管理人员，信息系统安全人员等）合作，为系统级别的连续监视建立适当的报告要求。 |
| T1004 | 使用持续监控工具持续评估风险。 |
| T1005 | 使用持续监控数据来制定信息安全投资决策以解决持续性问题。 |
| T1006 | 回应持续监测期间标记的问题，升级和协调回应。 |
| T1007 | 审查持续监测计划的结果并及时减少风险。 |

## A.5 NICE 框架知识描述

表 5 列出了直接应用于功能执行的各种信息。 详细工作角色中的每个工作角色都包含了此清单中选定的知识 ID /说明。附录 B 中列出。前六项对所有网络安全工作角色都是通用的。 此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 5 – NICE 框架知识描述**

| KSA ID | 描述 |
|---|---|
| K0001 | 计算机网络概念和协议知识，以及网络安全方法。 |
| K0002 | 了解风险管理流程（例如评估和减轻风险的方法）。 |
| K0003 | 了解与网络安全和隐私相关的法律，法规，政策和道德。 |
| K0004 | 了解网络安全和隐私原则。 |
| K0005 | 了解网络威胁和漏洞。 |
| K0006 | 了解网络安全失效的具体运营影响。 |
| K0007 | 有关认证，授权和访问控制方法的知识。 |
| K0008 | 了解适用的业务流程和客户组织的运作。 |
| K0009 | 了解应用程序漏洞。 |
| K0010 | 了解支持网络基础设施的通信方法，原理和概念。 |
| K0011 | 了解网络设备（包括路由器，交换机，网桥，服务器，传输介质和相关硬件）的功能和应用。 |
| K0012 | 了解功能和需求分析。 |

| | |
|---|---|
| K0013 | 了解网络防御和漏洞评估工具及其功能。 |
| K0014 | 了解复杂的数据结构。 |
| K0015 | 计算机算法知识。 |
| K0016 | 计算机编程原理知识 |
| K0017 | 处理数字取证数据的概念和实践的知识。 |
| K0018 | 加密算法的知识 |
| K0019 | 密码学知识和加密密钥管理概念 |
| K0020 | 了解数据管理和数据标准化政策。 |
| K0021 | 了解数据备份和恢复。 |
| K0022 | 有关数据挖掘和数据仓库原理的知识。 |
| K0023 | 了解数据库管理系统，查询语言，表关系和视图。 |
| K0024 | 了解数据库系统。 |
| K0025 | 数字权利管理知识。 |
| K0026 | 运营计划的业务连续性和灾难恢复连续性知识。 |
| K0027 | 了解组织的企业信息安全架构。 |
| K0028 | 了解组织的评估和验证要求。 |
| K0029 | 了解组织的本地和广域网连接。 |
| K0030 | 应用于计算机体系结构（如电路板，处理器，芯片和计算机硬件）的电气工程知识。 |
| K0031 | 了解企业消息传递系统和相关软件。 |
| K0032 | 了解弹性和冗余。 |
| K0033 | 主机/网络访问控制机制知识（例如，访问控制列表，功能列表）。 |
| K0034 | 了解提供网络通信的网络服务和协议交互。 |
| K0035 | 了解系统组件的安装，集成和优化。 |
| K0036 | 有关人机交互原理的知识。 |
| K0037 | 有关安全评估和授权过程的知识。 |
| K0038 | 用于管理与使用，处理，存储和传输信息或数据有关的风险的网络安全和隐私原理知识。 |
| K0039 | 了解适用于软件开发的网络安全和隐私原则和方法。 |

| | |
|---|---|
| K0040 | 了解漏洞信息传播来源（例如警报，建议，勘误和公告）。 |
| K0041 | 了解事件类别，事件响应和响应时间表。 |
| K0042 | 了解事件响应和处理方法。 |
| K0043 | 了解行业标准和组织认可的分析原理和方法。 |
| K0044 | 了解网络安全和隐私原则以及组织要求（与机密性，完整性，可用性，认证，不可否认性相关）。 |
| K0045 | 信息安全系统工程原理知识（NIST SP 800-160）。 |
| K0046 | 了解用于检测主机和基于网络的入侵的入侵检测方法和技术。 |
| K0047 | 有关信息技术（IT）架构概念和框架的知识。 |
| K0048 | 了解风险管理框架（RMF）的要求。 |
| K0049 | 了解信息技术（IT）安全原则和方法（例如防火墙，非军事区，加密）。 |
| K0050 | 了解局域网和广域网的原理和概念，包括带宽管理。 |
| K0051 | 对低级计算机语言（例如汇编语言）的了解。 |
| K0052 | 数学知识（如对数，三角，线性代数，微积分，统计和运算分析）。 |
| K0053 | 了解系统性能和可用性的度量或指标。 |
| K0054 | 通过使用基于标准的概念和功能评估，实施和传播信息技术（IT）安全评估，监测，检测和补救工具和程序的当前行业方法的知识。 |
| K0055 | 有关微处理器的知识。 |
| K0056 | 了解网络访问，身份和访问管理（例如公钥基础结构，Oauth，OpenID，SAML，SPML）。 |
| K0057 | 了解网络硬件设备和功能。 |
| K0058 | 网络流量分析方法的知识。 |
| K0059 | 了解新兴的信息技术（IT）和网络安全技术。 |
| K0060 | 操作系统知识。 |
| K0061 | 了解网络流量（如传输控制协议[TCP]和 Internet 协议[IP]，开放系统互连模型[OSI]，信息技术基础设施库，当前版本[ITIL]）的流量。 |
| K0062 | 了解数据包级分析。 |
| K0063 | 并行和分布式计算概念的知识。 |
| K0064 | 有关性能调整工具和技术的知识。 |

| | |
|---|---|
| K0065 | 了解基于策略和风险自适应访问控制。 |
| K0066 | 隐私影响评估的知识。 |
| K0067 | 过程工程概念的知识。 |
| K0068 | 有关编程语言结构和逻辑的知识。 |
| K0069 | 查询语言的知识，如 SQL（结构化查询语言）。 |
| K0070 | 了解系统和应用程序安全威胁和漏洞（例如缓冲区溢出，移动代码，跨站点脚本，程序语言/结构化查询语言[PL / SQL]和注入，竞争条件，隐蔽通道，重放，面向返回的攻击，恶意代码）。 |
| K0071 | 了解远程访问技术概念。 |
| K0072 | 了解资源管理原理和技术。 |
| K0073 | 了解安全配置管理技术。 （例如，安全技术实施指南（STIG），cisecurity.org 上的网络安全最佳实践）。 |
| K0074 | 了解安全管理中的关键概念（例如，发布管理，补丁管理）。 |
| K0075 | 安全系统设计工具，方法和技术的知识。 |
| K0076 | 有关服务器管理和系统工程理论，概念和方法的知识。 |
| K0077 | 了解服务器和客户端操作系统。 |
| K0078 | 了解服务器诊断工具和故障识别技术。 |
| K0079 | 有关软件调试原理的知识。 |
| K0080 | 软件设计工具，方法和技术的知识。 |
| K0081 | 软件开发模型的知识（例如，瀑布模型，螺旋模型）。 |
| K0082 | 软件工程知识。 |
| K0083 | 了解组织数据资产的来源，特征和用途。 |
| K0084 | 结构化分析原理和方法的知识。 |
| K0086 | 系统设计工具，方法和技术知识，包括自动化系统分析和设计工具。 |
| K0087 | 有关系统设计的系统软件和组织设计标准，政策和授权方法（例如国际标准化组织[ISO]指南）的知识。 |
| K0088 | 系统管理概念的知识。 |
| K0089 | 系统诊断工具和故障识别技术的知识。 |
| K0090 | 系统生命周期管理原理知识，包括软件安全性和可用性。 |

| | |
|---|---|
| K0091 | 系统测试和评估方法的知识。 |
| K0092 | 了解技术集成流程。 |
| K0093 | 电信概念知识（例如，通信信道，系统链路预算，频谱效率，多路复用）。 |
| K0094 | 了解与内容创建技术（例如，维基，社交网络，内容管理系统，博客）相关的功能和功能。 |
| K0095 | 了解与用于组织和管理信息的各种技术（例如，数据库，书签引擎）相关的功能和功能。 |
| K0096 | 了解各种协作技术（例如群件，SharePoint）的功能和功能。 |
| K0097 | 了解物理和虚拟数据存储介质的特性。 |
| K0098 | 了解网络防务服务提供商在自己的组织内的报告结构和流程。 |
| K0100 | 了解企业信息技术（IT）体系结构。 |
| K0101 | 了解组织的企业信息技术（IT）目标。 |
| K0102 | 了解系统工程过程。 |
| K0103 | 有关日常硬件维护的类型和频率的知识。 |
| K0104 | 有关虚拟专用网络（VPN）安全的知识。 |
| K0105 | Web 服务知识（例如，面向服务的体系结构，简单对象访问协议和 Web 服务描述语言）。 |
| K0106 | 了解构成网络攻击和网络攻击与威胁和漏洞之间关系的因素。 |
| K0107 | 知识内幕威胁调查，报告，调查工具和法律/法规。 |
| K0108 | 了解各种通信媒体（计算机和电话网络，卫星，光纤，无线）的概念，术语和操作。 |
| K0109 | 物理计算机组件和体系结构的知识，包括各种组件和外围设备（例如，CPU，网络接口卡，数据存储）的功能。 |
| K0110 | 对抗战术，技术和程序的知识。 |
| K0111 | 网络工具知识（例如 ping，traceroute，nslookup） |
| K0112 | 深入防御原理和网络安全体系结构的知识。 |
| K0113 | 了解不同类型的网络通信（例如 LAN，WAN，MAN，WLAN，WWAN）。 |

| | |
|---|---|
| K0114 | 电子设备（例如，计算机系统/组件，访问控制设备，数码相机，数字扫描仪，电子组织器，硬盘驱动器，存储卡，调制解调器，网络组件，联网设备，联网家庭控制设备，打印机，可移动存储设备，电话机，复印机，传真机等）。 |
| K0115 | 了解可以利用的技术。 |
| K0116 | 了解文件扩展名（例如，.dll，.bat，.zip，.pcap，.gzip）。 |
| K0117 | 有关文件系统实现（例如，新技术文件系统[NTFS]，文件分配表[FAT]，文件扩展名[EXT]）的知识。 |
| K0118 | 掌握和保存数字证据的流程知识。 |
| K0119 | 有关黑客方法的知识。 |
| K0120 | 了解信息需求和采集需求如何在扩展企业中进行翻译，跟踪和优先处理。 |
| K0121 | 了解信息安全计划管理和项目管理的原则和技巧。 |
| K0122 | 了解硬件，操作系统和网络技术的调查影响。 |
| K0123 | 有关可否受理的法律管理知识（例如证据规则）。 |
| K0124 | 了解多个认知领域以及适用于每个领域学习的工具和方法。 |
| K0125 | 了解收集，包装，运输和存储电子证据的流程，同时保持监管链。 |
| K0126 | 供应链风险管理实践知识（NIST SP 800-161） |
| K0127 | 了解相关信息结构的性质和功能（如国家信息基础设施）。 |
| K0128 | 了解持久性数据的类型和收集。 |
| K0129 | 有关命令行工具的知识（例如，mkdir，mv，ls，passwd，grep）。 |
| K0130 | 了解虚拟化技术和虚拟机的开发和维护。 |
| K0131 | 了解网络邮件收集，搜索/分析技术，工具和 cookie。 |
| K0132 | 了解哪些系统文件（例如，日志文件，注册表文件，配置文件）包含相关信息以及在哪里可以找到这些系统文件。 |
| K0133 | 了解数字取证数据的类型以及如何识别它们。 |
| K0134 | 可部署取证的知识。 |
| K0135 | 有关网页过滤技术的知识。 |
| K0136 | 了解不同电子通信系统和方法（例如电子邮件，VOIP，IM，网络论坛，直接视频广播）的功能。 |
| K0137 | 了解现有网络（例如，PBX，LAN，WAN，WIFI，SCADA）的范围。 |

| | |
|---|---|
| K0138 | 有关 Wi-Fi 的知识。 |
| K0139 | 对解释和编译的计算机语言的了解。 |
| K0140 | 有关安全编码技术的知识。 |
| K0141 | 撤回 - 集成到 K0420 中 |
| K0142 | 了解收集管理流程，功能和限制。 |
| K0143 | 了解前端收集系统，包括流量收集，过滤和选择。 |
| K0144 | 在全球范围内了解计算机攻击者的社会动态。 |
| K0145 | 了解安全事件关联工具。 |
| K0146 | 了解组织的核心业务/任务流程。 |
| K0147 | 了解新出现的安全问题，风险和漏洞。 |
| K0148 | 为减少供应链风险，了解进出口管制条例和责任机构。 |
| K0149 | 了解组织的风险承受能力和/或风险管理方法。 |
| K0150 | 了解企业事件响应计划，角色和责任。 |
| K0151 | 了解当前和新出现的威胁/威胁媒介。 |
| K0152 | 有关软件相关信息技术（IT）安全原则和方法（例如，模块化，分层，抽象，数据隐藏，简单/最小化）的知识。 |
| K0153 | 了解软件质量保证过程。 |
| K0154 | 了解供应链风险管理标准，流程和实践。 |
| K0155 | 有关电子证据法的知识。 |
| K0156 | 了解法律证据规则和法院程序。 |
| K0157 | 了解网络防御和信息安全政策，程序和法规。 |
| K0158 | 了解组织信息技术（IT）用户安全策略（例如帐户创建，密码规则，访问控制）。 |
| K0159 | IP 语音（VoIP）的知识。 |
| K0160 | 了解网络层上的常见攻击媒介。 |
| K0161 | 了解不同类型的攻击（例如，被动，主动，内部人员，近距离，分布式攻击）。 |
| K0162 | 网络攻击者的知识（例如脚本小子，内部威胁，非国家赞助，国家赞助）。 |
| K0163 | 关键信息技术（IT）采购要求的知识。 |

| | |
|---|---|
| K0164 | 有关功能，质量和安全要求的知识以及这些要求将如何应用于特定供应项目（即元素和过程）。 |
| K0165 | 了解风险/威胁评估。 |
| K0167 | 了解系统管理，网络和操作系统强化技术。 |
| K0168 | 有关适用法律，法规的知识（例如，美国法典第 10,18,32,50 条），总统指令，行政部门指导方针和/或行政/刑事法律指导方针和程序。 |
| K0169 | 了解信息技术（IT）供应链安全和供应链风险管理政策，要求和程序。 |
| K0170 | 使用信息通信技术的关键基础设施系统的知识，设计时没有系统安全考虑。 |
| K0171 | 硬件逆向工程技术知识。 |
| K0172 | 中间件知识（例如，企业服务总线和消息队列）。 |
| K0174 | 有关网络协议的知识。 |
| K0175 | 有关软件逆向工程技术的知识。 |
| K0176 | 了解可扩展标记语言（XML）模式。 |
| K0177 | 了解网络攻击阶段（例如，侦察，扫描，枚举，访问权限，特权升级，维护访问，网络开发，覆盖轨道）。 |
| K0178 | 了解安全软件部署方法，工具和实践。 |
| K0179 | 了解网络安全体系结构概念，包括拓扑，协议，组件和原理（例如应用纵深防御）。 |
| K0180 | 了解网络系统管理原理，模型，方法（例如，端到端系统性能监控）和工具。 |
| K0182 | 数据拆分工具和技术的知识（例如，最重要的）。 |
| K0183 | 逆向工程概念的知识。 |
| K0184 | 了解反辩证法的策略，技巧和程序。 |
| K0185 | 法医实验室设计配置和支持应用程序的知识（例如，VMWare，Wireshark）。 |
| K0186 | 调试程序和工具的知识。 |
| K0187 | 知道敌手对异常行为的文件类型滥用。 |
| K0188 | 有关恶意软件分析工具的知识（例如 Oily Debug，Ida Pro）。 |
| K0189 | 通过虚拟机检测（例如，虚拟感知恶意软件，调试器感知恶意软件和查找计算机显示设备中与虚拟机相关的字符串的解压缩恶意软件）了解恶意软件。 |
| K0190 | 了解加密方法。 |

| | |
|---|---|
| K0191 | 签名实施对病毒，恶意软件和攻击产生影响。 |
| K0192 | 有关 Windows / Unix 端口和服务的知识。 |
| K0193 | 了解数据库中的高级数据修复安全功能。 |
| K0194 | 了解基于云的知识管理技术和与安全，治理，采购和管理相关的概念。 |
| K0195 | 基于敏感性和其他风险因素的数据分类标准和方法的知识。 |
| K0196 | 有关密码学和其他安全技术的进出口法规知识。 |
| K0197 | 了解数据库访问应用程序编程接口（例如，Java 数据库连接[JDBC]）。 |
| K0198 | 有关组织过程改进概念和过程成熟度模型的知识（例如，用于开发的能力成熟度模型集成（CMMI），用于服务的 CMMI 和用于获取的 CMMI）。 |
| K0199 | 了解安全架构概念和企业架构参考模型（例如，Zachman，联邦企业架构[FEA]）。 |
| K0200 | 了解网络和相关标准的服务管理概念（例如，信息技术基础设施库，当前版本[ITIL]）。 |
| K0201 | 对称密钥旋转技术和概念的知识。 |
| K0202 | 了解应用程序防火墙的概念和功能（例如，单点认证/审计/策略实施，恶意内容的消息扫描，PCI 和 PII 合规性数据匿名化，数据丢失保护扫描，加速加密操作，SSL 安全性，REST / JSON 处理）。 |
| K0203 | 安全模型的知识（例如 Bell-LaPadula 模型，Biba 完整性模型，Clark Wilson 完整性模型）。 |
| K0204 | 学习评估技巧（评估，评估计划，测试，测验）的知识。 |
| K0205 | 了解基本系统，网络和操作系统强化技术。 |
| K0206 | 有关道德黑客原则和技术的知识。 |
| K0207 | 有关电路分析的知识。 |
| K0208 | 有关基于计算机的培训和电子学习服务的知识。 |
| K0209 | 隐秘通信技术的知识。 |
| K0210 | 了解数据备份和恢复概念。 |
| K0211 | 了解机密性，完整性和可用性要求。 |
| K0212 | 了解支持网络安全的软件产品。 |

| | |
|---|---|
| K0213 | 有关教学设计和评估模型的知识（例如，ADDIE，Smith / Ragan 模型，Gagne 的教学活动，Kirkpatrick 评估模型）。 |
| K0214 | 了解风险管理框架评估方法。 |
| K0215 | 了解组织培训政策。 |
| K0216 | 学习水平知识（即 Bloom 的学习分类学）。 |
| K0217 | 学习管理系统的知识及其在管理学习中的用途。 |
| K0218 | 学习风格的知识（例如，同化，听觉，动觉）。 |
| K0220 | 学习模式的知识（例如死记硬背，观察）。 |
| K0221 | 有关 OSI 模型和底层网络协议（如 TCP / IP）的知识。 |
| K0222 | 有关网络防御活动的相关法律，法律权限，限制和规定的知识。 |
| K0223 | 撤回 - 集成到 K0073 |
| K0224 | 熟悉操作系统的系统管理概念，例如但不限于 Unix / Linux，IOS，Android 和 Windows 操作系统。 |
| K0226 | 有关组织培训系统的知识。 |
| K0227 | 各种计算机体系结构的知识。 |
| K0228 | 有关分类学和语义本体论的知识。 |
| K0229 | 了解可以记录错误，异常和应用程序故障和日志记录的应用程序。 |
| K0230 | 了解云服务模型以及这些模型如何限制事件响应。 |
| K0231 | 了解危机管理协议，流程和技术。 |
| K0233 | 了解国家网络安全劳动力框架，工作角色和相关任务，知识，技能和能力。 |
| K0234 | 全面的网络能力（如防御，攻击，利用）的知识。 |
| K0235 | 了解如何利用研发中心，智库，学术研究和行业系统。 |
| K0236 | 了解如何利用 Hadoop，Java，Python，SQL，Hive 和 Pig 来探索数据。 |
| K0237 | 服务台行业最佳实践知识。 |
| K0238 | 有关机器学习理论和原理的知识。 |
| K0239 | 了解媒体制作，传播和传播技术和方法，包括通过书面，口头和视觉媒体进行宣传的替代方法。 |
| K0240 | 了解多级安全系统和跨域解决方案。 |
| K0241 | 了解组织人力资源政策，流程和程序。 |

| | |
|---|---|
| K0242 | 了解组织安全策略。 |
| K0243 | 了解组织培训和教育政策，流程和程序。 |
| K0244 | 了解可能表明可疑或异常活动的身体和生理行为。 |
| K0245 | 了解进行培训和教育需求评估的原则和流程。 |
| K0246 | 相关概念，程序，软件，设备和技术应用程序的知识。 |
| K0247 | 了解与客户支持相关的远程访问过程，工具和功能。 |
| K0248 | 战略理论和实践知识。 |
| K0249 | 有关维持技术，过程和战略的知识。 |
| K0250 | 有关学习者测试和评估流程的知识。 |
| K0251 | 了解司法程序，包括陈述事实和证据。 |
| K0252 | 有关课程设计的培训和教育原则和方法的知识，个人和群体的教学和指导以及培训和教育效果的衡量。 |
| K0253 | 撤回 - 集成到 K0227 中 |
| K0254 | 二元分析知识。 |
| K0255 | 了解网络体系结构概念，包括拓扑，协议和组件。 |
| K0257 | 了解信息技术（IT）采购/采购要求。 |
| K0258 | 测试程序，原则和方法的知识（例如，能力和成熟度模型集成（CMMI））。 |
| K0259 | 了解恶意软件分析概念和方法。 |
| K0260 | 了解个人身份信息（PII）数据安全标准。 |
| K0261 | 支付卡行业（PCI）数据安全标准的知识。 |
| K0262 | 了解个人健康信息（PHI）数据安全标准。 |
| K0263 | 了解信息技术（IT）风险管理政策，要求和程序。 |
| K0264 | 计划保护计划知识（例如信息技术（IT）供应链安全/风险管理政策，防篡改技术和要求）。 |
| K0265 | 了解基础设施支持信息技术（IT）的安全性，性能和可靠性。 |
| K0266 | 了解如何评估供应商和/或产品的可信度。 |
| K0267 | 了解与关键基础设施网络安全相关的法律，政策，程序或治理。 |
| K0268 | 法医足迹识别知识。 |
| K0269 | 移动通信体系结构知识。 |

| | |
|---|---|
| K0270 | 了解采购/采购生命周期过程。 |
| K0271 | 操作系统结构和内部知识（例如，进程管理，目录结构，安装的应用程序）。 |
| K0272 | 了解用于识别软件通信漏洞的网络分析工具。 |
| K0274 | 了解传输记录（例如蓝牙，射频识别（RFID），红外网络（IR），无线保真（Wi-Fi），寻呼，蜂窝，卫星天线，互联网语音协议（VoIP））以及干扰技术允许传输不需要的信息，或阻止已安装的系统正常运行。 |
| K0275 | 了解配置管理技术。 |
| K0276 | 安全管理知识。 |
| K0277 | 了解数据库中当前和新兴的数据加密（例如，列和表空间加密，文件和磁盘加密）安全功能（例如，内置加密密钥管理功能）。 |
| K0278 | 了解数据库中当前和新出现的数据修复安全功能。 |
| K0280 | 系统工程理论，概念和方法的知识。 |
| K0281 | 有关信息技术（IT）服务目录的知识。 |
| K0282 | 撤回 - 集成到 K0200 中 |
| K0283 | 了解与跨平台协作和内容同步有关的用例（例如，移动，PC，云）。 |
| K0284 | 有关开发和应用用户凭证管理系统的知识。 |
| K0285 | 实施企业密钥托管系统以支持静态数据加密的知识。 |
| K0286 | 有关 N 层类型的知识（例如包括服务器和客户端操作系统）。 |
| K0287 | 了解组织的信息分类程序和信息妥协程序。 |
| K0288 | 有关行业标准安全模型的知识。 |
| K0289 | 了解系统/服务器诊断工具和故障识别技术。 |
| K0290 | 系统安全测试和评估方法的知识。 |
| K0291 | 了解企业信息技术（IT）体系结构概念和模式（例如，基准，验证设计和目标体系结构）。 |
| K0292 | 有关事件，问题和事件管理的操作和流程的知识。 |
| K0293 | 将组织的目标和目标融入架构的知识。 |
| K0294 | 保持设备正常运行所需的 IT 系统操作，维护和安全知识。 |
| K0295 | 关于机密性，完整性和可用性原则的知识。 |

| | |
|---|---|
| K0296 | 了解网络设备（包括集线器，路由器，交换机，网桥，服务器，传输介质和相关硬件）的功能，应用程序和潜在的漏洞。 |
| K0297 | 识别安全风险的对策设计知识。 |
| K0298 | 了解确定的安全风险的对策。 |
| K0299 | 知道如何确定安全系统的工作原理（包括其弹性和可靠性能力）以及条件，操作或环境的变化如何影响这些结果。 |
| K0300 | 了解网络映射和重新创建网络拓扑。 |
| K0301 | 使用适当的工具（例如 Wireshark，tcpdump）了解数据包级分析。 |
| K0302 | 了解电脑的基本操作。 |
| K0303 | 有关使用子网工具的知识。 |
| K0304 | 处理数字取证数据的概念和实践的知识。 |
| K0305 | 数据隐藏知识（例如加密算法和速记）。 |
| K0308 | 知识密码学。 |
| K0309 | 掌握有潜力开发的新兴技术的知识。 |
| K0310 | 有关黑客方法的知识。 |
| K0311 | 了解有助于识别技术趋势的行业指标。 |
| K0312 | 了解情报收集原则，政策和程序，包括法律权限和限制。 |
| K0313 | 了解网络侧重点的外部组织和学术机构（如网络课程/培训和研究与开发）。 |
| K0314 | 了解行业技术潜在的网络安全漏洞。 |
| K0315 | 了解收集信息和制作，报告和分享信息的主要方法，程序和技巧。 |
| K0316 | 了解商业或军事行动计划，概念操作计划，订单，政策和参与规则。 |
| K0317 | 了解用于记录和查询报告事件，问题和事件的程序。 |
| K0318 | 有关操作系统命令行工具的知识。 |
| K0319 | 技术交付能力及其局限性知识。 |
| K0320 | 了解组织的评估和验证标准。 |
| K0321 | 应用于计算机体系结构和相关计算机硬件/软件的工程概念知识。 |
| K0322 | 嵌入式系统知识。 |
| K0323 | 了解系统容错方法。 |
| K0324 | 入侵检测系统（IDS）/入侵防御系统（IPS）工具和应用知识。 |

| | |
|---|---|
| K0325 | 信息理论知识（如信源编码，信道编码，算法复杂性理论和数据压缩）。 |
| K0326 | 非军事区知识。 |
| K0330 | 了解成功的能力以确定不太常见和更复杂的系统问题的解决方案。 |
| K0332 | 网络协议的知识，如 TCP / IP，动态主机配置，域名系统（DNS）和目录服务。 |
| K0333 | 了解网络设计流程，包括对安全目标，运营目标和权衡的理解。 |
| K0334 | 网络流量分析知识（工具，方法，流程）。 |
| K0335 | 了解当前和新兴的网络技术。 |
| K0336 | 有关访问认证方法的知识。 |
| K0337 | 撤回 - 集成到 K0007 |
| K0338 | 有关数据挖掘技术的知识。 |
| K0339 | 了解如何使用网络分析工具识别漏洞。 |
| K0340 | 了解与网络安全相关的外国信息披露政策和进出口管制条例。 |
| K0341 | 渗透测试原理，工具和技术的知识。 |
| K0342 | 了解根本原因分析技术。 |
| K0343 | 了解组织的威胁环境。 |
| K0344 | 有关集成系统组件的原理和方法的知识。 |
| K0347 | 对操作设计的了解和理解。 |
| K0349 | 了解网站类型，管理，功能和内容管理系统（CMS）。 |
| K0350 | 了解公认的组织规划体系。 |
| K0351 | 掌握有关网络定位和开发的适用法律，法律，法规和政策的知识。 |
| K0352 | 知识形式的情报支持需求，主题和重点领域。 |
| K0353 | 了解可能导致收款管理机构变更的情况。 |
| K0354 | 了解相关的报告和传播程序。 |
| K0355 | 了解所有来源的报告和传播程序。 |
| K0356 | 有关语言，语音和/或图形资料的分析工具和技术的知识。 |
| K0357 | 分析结构知识及其在评估操作环境中的用途。 |
| K0358 | 分析标准的知识和情报可信度的目的。 |
| K0359 | 获得批准的情报传播过程的知识。 |
| K0361 | 了解资产可用性，功能和限制。 |

| | |
|---|---|
| K0362 | 攻击方法和技术的知识（DDoS，蛮力，欺骗等）。 |
| K0363 | 了解审计和记录程序（包括基于服务器的记录）。 |
| K0364 | 了解评估适当收集任务所需的可用数据库和工具。 |
| K0367 | 渗透测试知识。 |
| K0368 | 掌握网络收集和/或准备活动的植入物的知识。 |
| K0371 | 了解收集开发过程的原则（例如拨号号码识别，社交网络分析）。 |
| K0372 | 编程概念知识（如层次，结构，编译与解释语言）。 |
| K0373 | 了解基本软件应用程序（例如数据存储和备份，数据库应用程序）以及这些应用程序中发现的漏洞类型。 |
| K0375 | 无线应用程序漏洞的知识。 |
| K0376 | 了解内部和外部客户及合作伙伴组织，包括信息需求，目标，结构，能力等。 |
| K0377 | 有关分类和控制标记标准，政策和程序的知识。 |
| K0379 | 客户组织的知识，包括信息需求，目标，结构，能力等。 |
| K0380 | 对协作工具和环境的了解。 |
| K0381 | 了解附带损害和估计影响。 |
| K0382 | 了解收集能力和限制。 |
| K0383 | 了解采集功能，访问，性能规格和用于满足采集计划的约束条件。 |
| K0384 | 了解收集管理功能（例如职位，职能，职责，产品，报告要求）。 |
| K0385 | 撤回 - 集成到 K0142 中 |
| K0386 | 有关收集管理工具的知识。 |
| K0387 | 有关收集计划过程和收集计划的知识。 |
| K0388 | 了解聊天/好友列表，新兴技术，VOIP，IP 电视，VPN，VSAT /无线，网络邮件和 cookies 的收集搜索/分析技术和工具。 |
| K0389 | 收集来源的知识，包括常规和非常规来源。 |
| K0390 | 有关收集策略的知识。 |
| K0391 | 了解收集系统，功能和流程。 |
| K0392 | 常见计算机/网络感染（病毒，木马等）和感染方法（端口，附件等）的知识。 |
| K0393 | 有关常见联网设备及其配置的知识。 |
| K0394 | 了解常见的报告数据库和工具。 |

| | |
|---|---|
| K0395 | 计算机网络基础知识（即网络的基本计算机组件，网络类型等）。 |
| K0396 | 计算机编程概念的知识，包括计算机语言，编程，测试，调试和文件类型。 |
| K0397 | 操作系统中安全概念的知识（例如，Linux，Unix）。 |
| K0398 | 与网站相关的概念知识（例如，网络服务器/网页，托管，DNS，注册，网页语言如 HTML）。 |
| K0399 | 了解危机行动计划和时间敏感的计划程序。 |
| K0400 | 有关网络行动危机行动规划的知识。 |
| K0401 | 了解评估收集产品的标准。 |
| K0402 | 关于目标选择和适用于网络领域的重要性和脆弱性因素（如价值，疗养，缓冲，对策）的知识。 |
| K0403 | 掌握密码学功能，限制和对网络操作的贡献。 |
| K0404 | 了解当前的收集要求。 |
| K0405 | 了解当前基于计算机的入侵集。 |
| K0406 | 了解当前用于主动防御和系统强化的软件和方法。 |
| K0407 | 了解客户信息需求。 |
| K0408 | 有关网络行动（即网络防御，信息收集，环境准备，网络攻击）原理，能力，限制和影响的知识。 |
| K0409 | 掌握网络情报/信息收集能力和知识库。 |
| K0410 | 网络法律知识及其对网络规划的影响。 |
| K0411 | 了解网络法律和法律考虑及其对网络规划的影响。 |
| K0412 | 网络词典/术语知识 |
| K0413 | 了解网络运营目标，政策和合法性。 |
| K0414 | 了解网络运营支持或启用流程。 |
| K0415 | 掌握网络操作术语/词汇。 |
| K0416 | 网络操作知识。 |
| K0417 | 有关数据通信术语（如网络协议，以太网，IP，加密，光学设备，可移动媒体）的知识。 |
| K0418 | 了解终端或环境收集的数据流程。 |
| K0419 | 有关数据库管理和维护的知识。 |

| | |
|---|---|
| K0420 | 数据库理论知识。 |
| K0421 | 有关数据库，门户网站和相关传播工具的知识。 |
| K0422 | 了解冲突过程和程序。 |
| K0423 | 了解解除冲突报告以包括外部组织的相互作用。 |
| K0424 | 了解拒绝和欺骗技巧。 |
| K0425 | 了解各级不同的组织目标，包括下级，侧级和更高级别。 |
| K0426 | 了解动态和有意识的定位。 |
| K0427 | 有关加密算法和网络功能/工具（如 SSL，PGP）的知识。 |
| K0428 | 了解无线局域网（WLAN）的加密算法和工具。 |
| K0429 | 了解企业级信息管理。 |
| K0430 | 逃避策略和技巧的知识。 |
| K0431 | 对不断发展/新兴通信技术的了解。 |
| K0432 | 了解与网络运营战略，政策和组织有关的现有，新兴和长期问题。 |
| K0433 | 掌握操作系统结构和操作的司法鉴定意义。 |
| K0435 | 对基本网络概念，原理，限制和影响的了解。 |
| K0436 | 掌握基本的网络操作概念，术语/词典（即环境准备，网络攻击，网络防御），原理，能力，限制和效果。 |
| K0437 | 通用监控和数据采集（SCADA）系统组件的知识。 |
| K0438 | 移动蜂窝通信架构（例如 LTE，CDMA，GSM / EDGE 和 UMTS / HSPA）的知识。 |
| K0439 | 掌握管理当局的知识。 |
| K0440 | 了解基于主机的安全产品以及这些产品如何影响开发和减少漏洞。 |
| K0442 | 了解融合技术如何影响网络运营（例如数字，电话，无线）。 |
| K0443 | 了解集线器，交换机和路由器如何在网络设计中一起工作。 |
| K0444 | 了解 Internet 应用程序如何工作（SMTP 电子邮件，基于 Web 的电子邮件，聊天客户端，VOIP）。 |
| K0445 | 了解现代数字和电话网络如何影响网络运营。 |
| K0446 | 了解现代无线通信系统如何影响网络运营。 |
| K0447 | 了解如何从元数据（例如电子邮件，http）收集，查看和识别感兴趣目标的重要信息。 |

| | |
|---|---|
| K0448 | 了解如何建立资源优先事项。 |
| K0449 | 了解如何提取，分析和使用元数据。 |
| K0450 | 撤回 - 集成到 K0036 中 |
| K0451 | 识别和报告流程的知识。 |
| K0452 | 了解实施提供半径认证和日志记录，DNS，邮件，Web 服务，FTP 服务器，DHCP，防火墙和 SNMP 的 Unix 和 Windows 系统的知识。 |
| K0453 | 有关适应症和警告的知识。 |
| K0454 | 了解信息需求。 |
| K0455 | 了解信息安全概念，促进技术和方法。 |
| K0456 | 有关情报能力和局限性的知识。 |
| K0457 | 了解情报的可信度。 |
| K0458 | 情报学科知识。 |
| K0459 | 了解情报就业要求（即后勤，通讯支持，可操作性，法律限制等）。 |
| K0460 | 了解情报准备环境和类似过程。 |
| K0461 | 情报生产过程的知识。 |
| K0462 | 了解情报报告原则，政策，程序和工具，包括报告格式，报告标准（要求和优先事项），传播实践以及法律权限和限制。 |
| K0463 | 智能需求任务系统的知识。 |
| K0464 | 智能支持计划，执行和评估。 |
| K0465 | 了解内部和外部合作伙伴网络运营能力和工具。 |
| K0466 | 了解内部和外部合作伙伴情报流程以及信息需求和基本信息的发展。 |
| K0467 | 了解内部和外部合作伙伴组织的能力和局限性（具有任务，收集，处理，利用和传播责任的组织）。 |
| K0468 | 了解内部和外部合作伙伴报告。 |
| K0469 | 了解预测和/或模拟威胁能力和行动的内部策略。 |
| K0470 | 互联网和路由协议的知识。 |
| K0471 | 互联网网络寻址知识（IP 地址，无类域间路由，TCP / UDP 端口编号）。 |
| K0472 | 入侵检测系统和签名开发知识。 |
| K0473 | 入侵集知识。 |

| | |
|---|---|
| K0474 | 关键的网络威胁参与者及其股票的知识。 |
| K0475 | 了解操作环境和威胁的关键因素。 |
| K0476 | 有关语言处理工具和技术的知识。 |
| K0477 | 了解领导力的意图和目标。 |
| K0478 | 了解定位时的法律考虑。 |
| K0479 | 了解恶意软件分析和特征。 |
| K0480 | 了解恶意软件。 |
| K0481 | 了解用于检测各种开采活动的方法和技术。 |
| K0482 | 了解确定收集资产状态和可用性的方法。 |
| K0483 | 了解整合和汇总来自任何潜在来源的信息的方法。 |
| K0484 | 了解中点收集（过程，目标，组织，目标等）。 |
| K0485 | 网络管理知识。 |
| K0486 | 了解网络结构和拓扑结构。 |
| K0487 | 网络安全知识（例如，加密，防火墙，认证，蜜罐，周界保护）。 |
| K0488 | 了解网络安全实施（例如，基于主机的 IDS，IPS，访问控制列表），包括其在网络中的功能和位置。 |
| K0489 | 网络拓扑知识。 |
| K0490 | 撤回 - 集成到 K0058 中 |
| K0491 | 网络和互联网通信基础知识（即设备，设备配置，硬件，软件，应用，端口/协议，寻址，网络架构和基础设施，路由，操作系统等）。 |
| K0492 | 了解非传统的收集方法。 |
| K0493 | 有关混淆技术的知识（例如，TOR /洋葱/匿名者，VPN / VPS，加密）。 |
| K0494 | 了解目标，情况，运营环境以及可用于支持规划的内部和外部合作伙伴收集能力的状态和处置。 |
| K0495 | 了解正在进行的和未来的行动。 |
| K0496 | 了解运营资产限制。 |
| K0497 | 运营效率评估知识。 |
| K0498 | 运营规划流程的知识。 |
| K0499 | 操作安全知识。 |

| | |
|---|---|
| K0500 | 有关组织和/或合作伙伴收集系统，能力和过程（例如收集和协议处理器）的知识。 |
| K0501 | 了解组织网络运营计划，战略和资源。 |
| K0502 | 了解组织决策支持工具和/或方法。 |
| K0503 | 了解资源和资产准备情况报告的组织形式，其操作相关性和情报收集影响。 |
| K0504 | 了解网络中的组织问题，目标和操作，以及管理网络操作的法规和政策指导。 |
| K0505 | 关于收集管理的组织目标和相关需求的知识。 |
| K0506 | 了解组织目标，领导优先级和决策风险。 |
| K0507 | 了解数字网络的组织或合作伙伴利用情况。 |
| K0508 | 了解与内部和/或外部组织合作的组织政策和规划概念。 |
| K0509 | 了解组织和合作伙伴的权力，责任和对实现目标的贡献。 |
| K0510 | 了解组织和合作伙伴政策，工具，能力和程序。 |
| K0511 | 了解组织层次结构和网络决策过程。 |
| K0512 | 组织规划概念的知识。 |
| K0513 | 了解组织优先级，法律部门和需求提交流程。 |
| K0514 | 了解组织结构和相关的情报能力。 |
| K0516 | 物理和逻辑网络设备和基础设施的知识，包括集线器，交换机，路由器，防火墙等。 |
| K0517 | 了解实施后审查（PIR）审批流程。 |
| K0518 | 计划活动启动的知识。 |
| K0519 | 了解计划时间表适应性，危机行动和时间敏感性计划。 |
| K0520 | 了解与目标发展有关的原则和实践，例如目标知识，协会，通信系统和基础设施。 |
| K0521 | 关于优先信息的知识，如何派生，如何发布，如何访问等 |
| K0522 | 生产开发和传播需求和架构的知识。 |
| K0523 | 了解主要供应商（例如，安全套件 - 趋势科技，赛门铁克，McAfee，Outpost 和 Panda）的产品和术语以及这些产品如何影响开发和减少漏洞。 |
| K0524 | 了解相关法律，法规和政策。 |
| K0525 | 掌握与网络运营计划相关的所需智能计划产品的知识。 |

| | |
|---|---|
| K0526 | 有关研究战略和知识管理的知识。 |
| K0527 | 了解风险管理和缓解策略。 |
| K0528 | 基于卫星的通信系统的知识。 |
| K0529 | 掌握脚本知识 |
| K0530 | 有关安全硬件和软件选项的知识，包括它们引发的网络人为因素及其对开发的影响。 |
| K0531 | 了解软件配置的安全含义。 |
| K0532 | 掌握专门的目标语言（例如，首字母缩略词，行话，技术术语，代码字）。 |
| K0533 | 了解特定的目标标识符及其用法。 |
| K0534 | 了解员工管理，分配和分配流程。 |
| K0535 | 有关目标研究的战略和工具的知识。 |
| K0536 | 了解开发工具（例如嗅探器，键盘记录器）和技术（例如，获得后门访问，收集/渗出数据，对网络中其他系统进行漏洞分析）的结构，方法和策略。 |
| K0538 | 了解目标和威胁组织结构，关键功能和关键漏洞 |
| K0539 | 了解目标通信配置文件及其关键要素（例如目标协会，活动，通信基础设施）。 |
| K0540 | 目标交流工具和技术的知识。 |
| K0541 | 有关目标文化参考，方言，表达，习语和缩写的知识。 |
| K0542 | 了解目标发展（即概念，角色，责任，产品等）。 |
| K0543 | 了解目标估计修复和恢复时间。 |
| K0544 | 了解目标情报收集和操作准备技术和生命周期。 |
| K0545 | 有关目标语言的知识。 |
| K0546 | 目标清单开发知识（即限制，联合，候选人等）。 |
| K0547 | 了解目标方法和程序。 |
| K0548 | 了解目标或威胁的网络行为者和程序。 |
| K0549 | 有关目标审查和验证程序的知识。 |
| K0550 | 有关目标的知识，包括相关的时事，交流情况，参与者和历史（语言，文化）和/或参考框架。 |
| K0551 | 了解定位周期。 |
| K0552 | 了解任务机制。 |

| | |
|---|---|
| K0553 | 了解有机和从属收集资产的任务流程。 |
| K0554 | 掌握任务，收集，处理，利用和传播的知识。 |
| K0555 | 了解 TCP / IP 网络协议。 |
| K0556 | 对电信基础知识的了解。 |
| K0557 | 有关终端或环境收集的知识（过程，目标，组织，目标等）。 |
| K0558 | 了解与收集要求和收集管理相关的可用工具和应用程序。 |
| K0559 | 了解融合应用的基本结构，体系结构和设计。 |
| K0560 | 了解现代通信网络的基本结构，架构和设计。 |
| K0561 | 掌握网络安全基础知识（例如，加密，防火墙，认证，蜜罐，周界防护）。 |
| K0562 | 了解新兴收集能力，访问和/或流程的功能和局限性。 |
| K0563 | 了解内部和外部馆藏适用于计划网络活动的能力，限制和任务方法。 |
| K0564 | 了解目标通信网络的特性（例如，容量，功能，路径，关键节点）。 |
| K0565 | 对常见网络和路由协议（例如 TCP / IP），服务（例如网络，邮件，DNS）的了解以及它们如何交互以提供网络通信。 |
| K0566 | 了解关键信息需求以及它们在计划中的用法。 |
| K0567 | 了解从收集来源到存储库和工具的数据流。 |
| K0568 | 了解收集管理和收集管理权限的定义。 |
| K0569 | 了解现有的任务，收集，处理，利用和传播架构。 |
| K0570 | 了解可能影响收集操作的威胁因素。 |
| K0571 | 了解收集过程中的反馈周期。 |
| K0572 | 了解模拟威胁活动以使组织受益的内部团队的功能和能力。 |
| K0573 | 了解数字取证的基本原理以提取可操作的情报。 |
| K0574 | 了解语言分析对网上操作员功能的影响。 |
| K0575 | 了解内部和外部合作伙伴人员配置估算的影响。 |
| K0576 | 了解信息环境。 |
| K0577 | 了解情报框架，流程和相关系统。 |
| K0578 | 了解情报需求的发展和对信息处理的要求。 |
| K0579 | 了解更高，更低和相邻子元素的组织，角色和责任。 |
| K0580 | 了解组织收集计划的既定格式。 |

| | |
|---|---|
| K0581 | 了解组织的计划，运营和定位周期。 |
| K0582 | 了解组织规划和人员配置过程。 |
| K0583 | 了解描述目标的组织计划/指示/指导。 |
| K0584 | 有关临时转让征收权的组织政策/程序的知识。 |
| K0585 | 与全面网络运营相关的组织结构知识，包括职能，责任和不同内部因素之间的相互关系。 |
| K0586 | 了解行动过程和运动分析的结果。 |
| K0587 | 了解建立环境准备和监督产品所需的 POC，数据库，工具和应用程序。 |
| K0588 | 了解组织的下级，侧级和更高级别的优先级信息要求。 |
| K0589 | 了解用于评估运营绩效和影响的流程。 |
| K0590 | 了解将操作评估程序与关键信息需求过程同步的过程。 |
| K0591 | 了解生产责任和有机分析和生产能力。 |
| K0592 | 了解目标模板的目的和贡献。 |
| K0593 | 了解网络行动的范围及其潜在的情报支持需求，主题和重点领域。 |
| K0594 | 了解最终状态，目标，效果，操作线等之间的关系。 |
| K0595 | 了解操作目标，情报需求和情报生产任务之间的关系。 |
| K0596 | 解信息处理的请求。 |
| K0597 | 了解网络运营在支持和促进其他组织运营方面的作用。 |
| K0598 | 了解组织特定计划，指导和授权的结构和意图。 |
| K0599 | 了解现代数字和电话网络的结构，体系结构和设计。 |
| K0600 | 了解现代无线通信系统的结构，体系结构和设计。 |
| K0601 | 了解用于协调的系统/架构/通信。 |
| K0602 | 有关收集规范和能力的知识。 |
| K0603 | 了解目标或威胁使用互联网的方式。 |
| K0604 | 了解威胁和/或目标系统。 |
| K0605 | 知识的小费，提示，混合和冗余。 |
| K0606 | 转录知识开发过程和技术（例如，逐字，要旨，摘要）的。 |
| K0607 | 了解翻译过程和技术。 |

| | |
|---|---|
| K0608 | 熟悉 Unix / Linux 和 Windows 操作系统的结构和内部（例如，进程管理，目录结构，安装的应用程序）。 |
| K0609 | 了解虚拟机技术。 |
| K0610 | 了解虚拟化产品（VMware，Virtual PC）。 |
| K0611 | 撤回 - 集成到 K0131 中 |
| K0612 | 了解什么构成对网络的“威胁”。 |
| K0613 | 了解组织的运营规划人员，联系方式和联系方式，以及他们的期望。 |
| K0614 | 无线技术（例如，蜂窝，卫星，GSM）的知识包括现代无线通信系统的基本结构，体系结构和设计。 |
| K0615 | 根据现行法律了解隐私披露声明。 |
| K0616 | 持续监测知识，过程以及持续诊断和缓解（CDM）计划活动。 |
| K0617 | 自动化安全控制评估知识 |
| K0618 | 硬件资产管理知识以及跨部门，地点和设施跟踪联网设备和软件的位置和配置以及可能支持业务功能的价值。 |
| K0619 | 了解软件资产管理以及跨部门，地点和设施跟踪联网设备和软件的位置和配置以及潜在地支持业务功能的价值。 |
| K0620 | 持续监测技术和工具的知识。 |
| K0621 | 了解风险评分。 |
| K0622 | 掌握与使用，处理，存储和传输数据有关的控制知识。 |
| K0623 | 了解风险评估方法。 |
| K0624 | 应用程序安全风险知识（例如，开放式 Web 应用程序安全性项目前 10 名） |
| K0625 | 对于某些网络设备来说，修补和软件更新是不切实际的。 |
| K0626 | 了解安全更新机制。 |
| K0627 | 了解入口过滤对防止依赖欺骗网络地址的自动化威胁的重要性。 |
| K0628 | 通过在模拟的现实世界中提供实践经验，将网络竞赛作为发展技能的一种方式的知识。 |
| K0629 | 白/黑名单的知识 |
| K0630 | 了解最新的入侵技术，方法和组织外部的入侵记录。 |

## A.6 NICE 框架技能描述

表 6 列出了网络安全技能。 技能是执行学习的精神运动行为的可观察的能力。 附录 B 列出了详细工作角色中每个工作角色的列表中选择的技能描述。此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 6 – NICE 框架技能描述**

| 技能 ID | 描述 |
|---|---|
| S0001 | 进行漏洞扫描和识别安全系统漏洞方面的技能。 |
| S0002 | 数据管理系统设计中分配存储容量的技能。 |
| S0003 | 识别，捕获，包含和报告恶意软件的技巧。 |
| S0004 | 分析网络流量和性能特点的技巧。 |
| S0005 | 将信息技术应用于所提议的解决方案的技能。 |
| S0006 | 熟练运用机密性，完整性和可用性原则。 |
| S0007 | 应用主机/网络访问控制（例如访问控制列表）的技巧。 |
| S0008 | 熟练应用组织特定的系统分析原理和技术。 |
| S0009 | 熟练评估安全系统和设计的稳健性。 |
| S0010 | 进行能力和需求分析的技能。 |
| S0011 | 进行信息搜索技能。 |
| S0012 | 进行知识映射的技能（例如知识库地图）。 |
| S0013 | 熟练进行查询和开发算法来分析数据结构。 |
| S0014 | 熟练进行软件调试。 |
| S0015 | 进行测试活动的技能。 |
| S0016 | 熟练配置和优化软件。 |
| S0017 | 创建和利用数学或统计模型的技能。 |
| S0018 | 创建反映系统安全目标的策略的技能。 |
| S0019 | 创建验证和处理多个输入的程序，包括命令行参数，环境变量和输入流的技能。 |
| S0020 | 开发和部署签名的技能。 |
| S0021 | 在设计数据分析结构（即测试必须产生的数据类型以及如何分析数据）方面的技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0022 | 设计对策确定安全风险的技能。 |
| S0023 | 基于网络安全原则和原则设计安全控制的技能。 |
| S0024 | 设计硬件和软件解决方案的集成的技能。 |
| S0025 | 通过入侵检测技术（例如 Snort）检测基于主机和网络的入侵的技巧。 |
| S0026 | 确定给定系统的适当测试严格等级的技能。 |
| S0027 | 确定安全系统应该如何工作的技巧（包括其弹性和可靠性能力）以及条件，操作或环境的变化如何影响这些结果。 |
| S0028 | 熟练开发数据字典。 |
| S0029 | 熟练开发数据模型。 |
| S0030 | 熟练开发基于操作的测试场景。 |
| S0031 | 在开发和应用安全系统访问控制的技能。 |
| S0032 | 熟练开发，测试和实施网络基础设施应急和恢复计划。 |
| S0033 | 诊断连接问题的技巧。 |
| S0034 | 识别信息系统和网络的保护需求（即安全控制）的技能。 |
| S0035 | 建立路由模式的技巧。 |
| S0036 | 评估安全设计是否充分的技巧。 |
| S0037 | 生成查询和报告的技巧。 |
| S0038 | 识别相对于系统目标的系统性能的度量或指标以及改进或纠正性能所需的行动的技能。 |
| S0039 | 识别可能导致系统性能或可用性降低的原因的技能，并开始采取必要行动来缓解这种恶化。 |
| S0040 | 实施，维护和改进已建立的网络安全实践的技能。 |
| S0041 | 熟练安装，配置和排除 LAN 和 WAN 组件，如路由器，集线器和交换机。 |
| S0042 | 维护数据库的技能。 （即备份，恢复，删除数据，事务日志文件等）。 |
| S0043 | 维护目录服务的技能。 （例如，Microsoft Active Directory，LDAP 等）。 |
| S0044 | 模仿威胁行为的技巧。 |
| S0045 | 优化数据库性能的技巧。 |

| 技能 ID | 描述 |
| --- | --- |
| S0046 | 使用适当的工具（例如 Wireshark，tcpdump）进行数据包级分析的技巧。 |
| S0047 | 根据标准操作程序或国家标准保持证据完整性的技能。 |
| S0048 | 系统集成测试中的技能。 |
| S0049 | 测量和报告知识资本的技能。 |
| S0050 | 熟练掌握设计建模和构建用例（如统一建模语言）。 |
| S0051 | 熟练使用渗透测试工具和技术。 |
| S0052 | 使用社会工程技术的技能。 （例如，钓鱼，诱饵，尾随等）。 |
| S0053 | 调整传感器的技巧。 |
| S0054 | 熟练使用事件处理方法。 |
| S0055 | 使用知识管理技术的技能。 |
| S0056 | 熟练使用网络管理工具分析网络流量模式（例如简单的网络管理协议）。 |
| S0057 | 使用协议分析器的技巧。 |
| S0058 | 熟练使用适当的工具修复系统的软件，硬件和外围设备。 |
| S0059 | 使用虚拟专用网络（VPN）设备和加密的技巧。 |
| S0060 | 用当前支持的编程语言（例如 Java，C ++）编写代码的技巧。 |
| S0061 | 编写测试计划的技巧。 |
| S0062 | 分析内存转储以提取信息的技巧。 |
| S0063 | 从各种网络防御资源收集数据的技能。 |
| S0064 | 开发和执行技术培训计划和课程的技能。 |
| S0065 | 识别和提取不同媒体法医兴趣数据的技能（即媒体法医学）。 |
| S0066 | 确定技术能力方面差距的技能。 |
| S0067 | 熟练使用 Windows，Unix 或 Linux（例如，密码，用户帐户，文件）识别，修改和操作适用的系统组件。 |
| S0068 | 收集，处理，包装，运输和存储电子证据的技能，以避免更改，丢失，物理损坏或数据破坏。 |
| S0069 | 设立电子数据鉴定的工作站技能。 |
| S0070 | 与他人交谈以有效传达信息的技巧。 |

| 技能 ID | 描述 |
| --- | --- |
| S0071 | 熟练使用司法取证工具套件（例如 EnCase，Sleuthkit，FTK）。 |
| S0072 | 使用科学规则和方法解决问题的技巧。 |
| S0073 | 熟练使用虚拟机。（例如，Microsoft Hyper-V，VMWare vSphere，Citrix XenDesktop / Server，Amazon Elastic Compute Cloud 等）。 |
| S0074 | 物理拆卸个人电脑的技能。 |
| S0075 | 在多种操作系统环境（例如移动设备系统）中进行取证分析的技能。 |
| S0076 | 熟练配置和使用基于软件的计算机保护工具（例如，软件防火墙，防病毒软件，反间谍软件）。 |
| S0077 | 确保网络通信的技巧。 |
| S0078 | 识别和分类漏洞类型和相关的攻击的技能。 |
| S0079 | 保护网络免受恶意软件侵害的技巧。（例如，NIPS，反恶意软件，限制/阻止外部设备，垃圾邮件过滤器）。 |
| S0080 | 进行损害评估的技能。 |
| S0081 | 使用网络分析工具识别漏洞的技巧。 （例如，模糊，nmap 等）。 |
| S0082 | 熟练评估测试计划的适用性和完整性。 |
| S0083 | 将黑盒安全测试工具集成到软件发布的质量保证过程中的技巧。 |
| S0084 | 熟练配置和使用网络保护组件（例如，防火墙，VPN，网络入侵检测系统）。 |
| S0085 | 技术人员对技术系统进行审核或评审。 |
| S0086 | 评估供应商和/或产品的可信度的技能。 |
| S0087 | 深入分析捕获的恶意代码的技巧（例如恶意软件取证）。 |
| S0088 | 熟练使用二进制分析工具（例如 Hexedit，命令代码 xxd，hexdump）。 |
| S0089 | 在单向散列函数中的技巧（例如，安全散列算法[SHA]，消息摘要算法[MD5]）。 |
| S0090 | 将异常代码分析为恶意或良性的技巧。 |
| S0091 | 分析易失数据的技巧。 |
| S0092 | 识别混淆技巧的技巧。 |
| S0093 | 熟练解释调试器的结果以确定策略，技术和程序。 |
| S0094 | 阅读十六进制数据的技巧。 |

| 技能 ID | 描述 |
| --- | --- |
| S0095 | 识别常见编码技术（例如，Exclusive Disjunction [XOR]，美国信息交换标准码 [ASCII]，Unicode，Base64，Uuencode，统一资源定位符[URL]编码）的技能。 |
| S0096 | 阅读和解读签名的技巧（如 snort）。 |
| S0097 | 应用安全控制技能。 |
| S0100 | 利用或开发学习活动的技巧（如情景，教学游戏，互动练习）。 |
| S0101 | 利用技术（例如，SmartBoards，网站，电脑，投影仪）用于教学目的的技术。 |
| S0102 | 运用技术交付能力的技巧。 |
| S0103 | 评估模型的预测能力和随后的普遍性的技巧。 |
| S0104 | 进行测试准备评审的技能。 |
| S0106 | 数据预处理（例如，插补，降维，归一化，转换，提取，过滤，平滑）的技巧。 |
| S0107 | 技能设计和记录整体方案测试和评估策略。 |
| S0108 | 熟练开发员工队伍和职位资格标准。 |
| S0109 | 识别隐藏模式或关系的技巧。 |
| S0110 | 识别测试和评估基础设施（人员，范围，工具，仪器）要求的技能。 |
| S0111 | 与客户沟通的技巧。 |
| S0112 | 熟练管理测试资产，测试资源和测试人员，以确保有效完成测试事件。 |
| S0113 | 执行格式转换来创建数据的标准表示技巧。 |
| S0114 | 熟练进行敏感性分析。 |
| S0115 | 熟练准备测试和评估报告。 |
| S0116 | 设计多级安全/跨域解决方案的技能。 |
| S0117 | 提供测试和评估资源估算的技能。 |
| S0118 | 熟练开发机器可理解的语义本体。 |
| S0119 | 回归分析中的技巧（例如，分层逐步，广义线性模型，普通最小二乘，基于树的方法，逻辑）。 |
| S0120 | 审查日志以确定过去入侵证据的技能。 |
| S0121 | 熟练使用系统，网络和操作系统强化技术。 （例如，移除不必要的服务，密码策略，网络分段，启用日志记录，最小权限等）。 |

| 技能 ID | 描述 |
| --- | --- |
| S0122 | 熟练使用设计方法。 |
| S0123 | 转化分析技能（例如，汇总，丰富，处理）。 |
| S0124 | 熟练解决和诊断网络防御基础设施异常并解决问题。 |
| S0125 | 熟练使用基本的描述性统计和技术（例如，正态性，模型分布，散点图）。 |
| S0126 | 熟练使用数据分析工具（如 Excel，STATA SAS，SPSS）。 |
| S0127 | 熟练使用数据映射工具。 |
| S0128 | 熟练使用人力和人事 IT 系统。 |
| S0129 | 使用异常值识别和清除技术的技巧。 |
| S0130 | 使用 R，Python，PIG，HIVE，SQL 等编写脚本的技巧 |
| S0131 | 分析恶意软件的技巧。 |
| S0132 | 进行 Bit 级分析技能。 |
| S0133 | 处理数字证据的技能，包括保护和制作合法的证据副本。 |
| S0134 | 执行系统评估技术。 |
| S0135 | 熟悉安全测试计划设计（例如，单元，集成，系统，验收）。 |
| S0136 | 网络系统管理原理，模型，方法（例如，端到端系统性能监控）和工具的技能。 |
| S0137 | 进行应用程序漏洞评估的技能。 |
| S0138 | 熟练使用公钥基础设施（PKI）加密和数字签名功能进入应用程序（例如 S / MIME 电子邮件，SSL 流量）。 |
| S0139 | 应用安全模型的技巧（例如 Bell-LaPadula 模型，Biba 完整模型，Clark Wilson 完整模型）。 |
| S0140 | 熟练应用系统工程过程。 |
| S0141 | 熟练评估安全系统设计。 |
| S0142 | 技术人员进行研究以解决新的客户端问题。 |
| S0143 | 进行系统/服务器规划，管理和维护的技能。 |
| S0144 | 能够纠正影响系统/服务器性能的物理和技术问题。 |
| S0145 | 技术整合和应用符合系统安全目标的策略。 |
| S0146 | 技术创建使系统达到性能目标（例如流量路由，SLA，CPU 规格）的策略。 |

| 技能 ID | 描述 |
| --- | --- |
| S0147 | 根据网络安全原则和原则评估安全控制的技能。 （例如，CIS CSC，NIST SP 800-53，网络安全框架等）。 |
| S0148 | 技术设计技术流程和解决方案的整合，包括遗留系统和现代编程语言。 |
| S0149 | 熟练开发可以记录和处理错误，异常和应用程序错误和日志记录的应用程序。 |
| S0150 | 具备实施和测试网络基础设施应急和恢复计划的技能。 |
| S0151 | 对故障系统组件（即服务器）进行故障排除的技巧 |
| S0152 | 将操作要求转换为保护需求（即安全控制）的技能。 |
| S0153 | 识别和预测系统/服务器性能，可用性，容量或配置问题的技能。 |
| S0154 | 熟练安装系统和组件升级。 （即服务器，设备，网络设备）。 |
| S0155 | 技能监控和优化系统/服务器性能。 |
| S0156 | 执行数据包级分析技能。 |
| S0157 | 恢复故障系统/服务器的技巧。 （例如，恢复软件，故障转移群集，复制等）。 |
| S0158 | 操作系统管理的技巧。 （例如账户维护，数据备份，维护系统性能，安装和配置新的硬件/软件）。 |
| S0159 | 根据批准的标准和/或规范，配置和验证网络工作站和外围设备。 |
| S0160 | 熟练使用设计建模（例如统一建模语言）。 |
| S0161 | 撤回 - 集成到 S0160 |
| S0162 | 子网技巧。 |
| S0163 | 已撤销 - 已纳入 S0060 S0164 评估密码标准应用的技能。 |
| S0164 | 评估密码标准应用的技能。 |
| S0166 | 确定技术交付能力方面的差距的技能。 |
| S0167 | 技能识别安全系统中的漏洞。 （例如，漏洞和合规性扫描）。 |
| S0168 | 擅长设置将内部局域网（LAN）与其他不受信任的网络隔开的物理或逻辑子网。 |
| S0169 | 进行趋势分析的技能。 |
| S0170 | 熟练配置和使用计算机保护组件（如适当的硬件防火墙，服务器，路由器）。 |
| S0171 | 执行影响/风险评估的技能。 |
| S0172 | 使用安全编码技术的技巧。 |

| 技能 ID | 描述 |
| --- | --- |
| S0173 | 熟练使用安全事件关联工具。 |
| S0174 | 熟练使用代码分析工具。 |
| S0175 | 执行根源分析的技能。 |
| S0176 | 行政规划活动的技能，包括准备功能和具体的支持计划，准备和管理通信以及人员配置程序。 |
| S0177 | 分析目标通信网络的技巧。 |
| S0178 | 分析基本网络数据（例如路由器配置文件，路由协议）的技巧。 |
| S0179 | 分析语言处理工具的技巧，提供反馈以加强工具开发。 |
| S0180 | 撤回 - 集成到 S0062 |
| S0181 | 分析事件进程中收集数据的技巧。 |
| S0182 | 分析从无线局域网收集的目标通信内部和外部的技巧。 |
| S0183 | 分析终端或环境收集数据的技能。 |
| S0184 | 分析流量以识别网络设备的技巧。 |
| S0185 | 应用分析方法的技巧，通常用于支持规划并证明推荐的策略和行动路线是合理的。 |
| S0186 | 应用危机计划程序的技巧。 |
| S0187 | 应用各种分析方法，工具和技术的技巧（如竞争性假设;推理链;情景方法;拒绝和欺骗检测;高影响低概率;网络/关联或链接分析;贝叶斯，德尔福和模式分析） 。 |
| S0188 | 评估目标的参照系（例如，动机，技术能力，组织结构，敏感性）的技能。 |
| S0189 | 评估和/或评估网络操作期间和之后产生的影响的技能。 |
| S0190 | 评估当前工具以识别所需改进的技巧。 |
| S0191 | 评估现有分析工具适用于各种情况的技能。 |
| S0192 | 熟练审计防火墙，周界，路由器和入侵检测系统。 |
| S0193 | 符合针对性信息的法律限制的技能。 |
| S0194 | 进行非归属研究的技能。 |
| S0195 | 使用所有可用来源进行研究的技能。 |
| S0196 | 使用暗网进行研究的技巧。 |

| 技能 ID | 描述 |
| --- | --- |
| S0197 | 在进行社交网络分析，好友列表分析和/或 cookie 分析方面的技能。 |
| S0198 | 进行社交网络分析的技能。 |
| S0199 | 从数据包捕获中创建和提取重要信息的技能。 |
| S0200 | 创建采集需求以支持数据采集活动的技能。 |
| S0201 | 创造支持远程操作计划的技能。（即热/暖/冷/替代站点，灾难恢复）。 |
| S0202 | 熟练掌握数据挖掘技术（如搜索文件系统）和分析。 |
| S0203 | 定义和操作环境特征所有相关方面的技能。 |
| S0204 | 描绘网络地图上的来源或附属资料的技巧。 |
| S0205 | 通过评估可用功能与预期效果来确定适当的定位选项的技能。 |
| S0206 | 熟练掌握各种操作系统上已安装的补丁和识别补丁签名。 |
| S0207 | 熟悉各种路由器和防火墙配置对 LAN 和 WAN 环境中的流量模式和网络性能的影响。 |
| S0208 | 确定网络设备的物理位置的技巧。 |
| S0209 | 熟练开发和执行全面的网络操作评估程序，以评估和验证操作性能特征。 |
| S0210 | 开发情报报告的技能。 |
| S0211 | 有能力开发或推荐分析方法或解决信息不完整或无先例存在的问题和情况。 |
| S0212 | 及时传播智力最高的物品的技能。 |
| S0213 | 记录和传达复杂的技术和程序化信息的技巧。 |
| S0214 | 评估获取知识价值的技能。 |
| S0215 | 评估和解释元数据的技巧。 |
| S0216 | 评估可用功能与预期效果，以提供有效的行动方案的技能。 |
| S0217 | 熟练掌握相关性，可靠性和客观性的数据来源。 |
| S0218 | 评估信息的可靠性，有效性和相关性方面的技能。 |
| S0219 | 评估信息以识别相关性，优先级等方面的技巧 |
| S0220 | 熟练利用/查询组织和/或合作伙伴收集数据库。 |
| S0221 | 从数据包捕获中提取信息的技巧。 |
| S0222 | 融合分析技能 |
| S0223 | 制定运营计划以支持任务和目标要求的技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0224 | 熟悉目标通信的技巧。 |
| S0225 | 识别目标通信网络的技能。 |
| S0226 | 识别目标网络特征的技能。 |
| S0227 | 识别替代解析解释以减少意外结果的技巧。 |
| S0228 | 识别关键目标元素的技能，包括网络领域的关键目标元素。 |
| S0229 | 识别可能危及组织和/或合作伙伴利益的网络威胁的技能。 |
| S0230 | 已撤销 - 已纳入 S0066 |
| S0231 | 识别目标如何沟通的技巧。 |
| S0232 | 识别智力差距和局限性的技巧。 |
| S0233 | 识别可能影响组织目标的语言问题。 |
| S0234 | 确定导致目标发展的技能。 |
| S0235 | 识别非目标区域语言和方言的技巧 |
| S0236 | 识别在协议模型的每个级别工作的设备的技能。 |
| S0237 | 通过地理空间分析技术识别，定位和跟踪目标的技能 |
| S0238 | 信息优先排序技能与运营相关。 |
| S0239 | 熟练编译和解释编程语言。 |
| S0240 | 解释收集系统所应用的元数据和内容的技巧。 |
| S0241 | 解释 traceroute 结果的技巧，因为它们适用于网络分析和重建。 |
| S0242 | 解读漏洞扫描器结果的技巧来识别漏洞。 |
| S0243 | 知识管理技巧，包括技术文档技术（例如维基页面）。 |
| S0244 | 掌握客户关系管理的技巧，包括确定客户需求/要求，管理客户期望以及展示对提供高质量结果的承诺。 |
| S0245 | 浏览网络可视化软件的技巧。 |
| S0246 | 数字正常化的技能。 |
| S0247 | 利用现有情报进行数据融合的技巧，以实现新的持续收集。 |
| S0248 | 熟练执行目标系统分析。 |
| S0249 | 编制和提交简报的技能 |

| 技能 ID | 描述 |
| --- | --- |
| S0250 | 准备计划和相关信函的技能。 |
| S0251 | 优先考虑目标语言材料的技巧。 |
| S0252 | 处理收集的数据以便进行后续分析。 |
| S0253 | 提供有关目标相关问题（如语言，文化，交流）的分析的技能。 |
| S0254 | 提供分析，以协助在行动报告后分阶段撰写的技能。 |
| S0255 | 利用目标基础设施提供实时，可操作的地理位置信息的技巧。 |
| S0256 | 通过对物理，功能或行为关系的识别和链接分析，提供对目标或威胁系统的理解方面的技能。 |
| S0257 | 在 Windows 和 Unix 系统（例如执行分析大型数据文件，自动执行手动任务以及获取/处理远程数据等任务的人员）阅读，解释，编写，修改和执行简单脚本（例如 PERL，VBS） 。 |
| S0258 | 识别和解释流量中的恶意网络活动的技能。 |
| S0259 | 识别目标的拒绝和欺骗技术的技能。 |
| S0260 | 识别中点机会和重要信息的技巧。 |
| S0261 | 识别信息相关性的技巧。 |
| S0262 | 识别目标通信模式的重大变化的技能。 |
| S0263 | 识别可能用于元数据分析的潜在客户的技术信息的技能。 |
| S0264 | 熟练掌握技术信息，可用于指导远程操作（数据包括用户，密码，电子邮件地址，目标的 IP 范围，DNI 行为频率，邮件服务器，域服务器，SMTP 标头信息）。 |
| S0265 | 识别技术信息的技能，可用于包括智力开发在内的目标开发。 |
| S0266 | 熟练使用相关的编程语言（例如 C ++，Python 等）。 |
| S0267 | 熟练掌握远程命令行和图形用户界面（GUI）工具的用法。 |
| S0268 | 研究基本信息的技能。 |
| S0269 | 技术研究流量中使用的漏洞和缺陷。 |
| S0270 | 逆向工程技巧（例如，十六进制编辑，二进制打包实用程序，调试和字符串分析）来识别远程工具的功能和所有权。 |
| S0271 | 熟练审查和编辑评估产品。 |
| S0272 | 熟练阅读和编辑来自网络操作各种来源的情报产品。 |

| 技能 ID | 描述 |
| --- | --- |
| S0273 | 熟练审查和编辑计划。 |
| S0274 | 熟练审查和编辑目标材料。 |
| S0275 | 服务器管理的技能。 |
| S0276 | 熟练掌握无线局域网元数据的调查，收集和分析。 |
| S0277 | 跨数据集合成，分析和优先化意义上的技能。 |
| S0278 | 在将分析调整到必要水平（例如分类和组织）方面的技巧。 |
| S0279 | 直接支持收集操作的目标开发技能。 |
| S0280 | 熟悉目标网络异常识别（例如入侵，数据流或处理，目标实施新技术）。 |
| S0281 | 技术写作技巧。 |
| S0282 | 技能测试和评估实施工具。 |
| S0283 | 熟练抄录目标语言沟通。 |
| S0284 | 翻译目标图形和/或语音材料的技巧。 |
| S0285 | 使用布尔运算符构建简单和复杂的查询的技巧。 |
| S0286 | 使用数据库识别目标相关信息的技巧。 |
| S0287 | 熟练使用地理空间数据和应用地理空间资源。 |
| S0288 | 使用多种分析工具，数据库和技术（例如 Analyst's Notebook，A-Space，Anchory，M3，divergent / convergent thinking，链接图，矩阵等）的技巧。 |
| S0289 | 使用多个搜索引擎（例如 Google，Yahoo，LexisNexis，DataStar）和工具来进行开源搜索的技巧。 |
| S0290 | 使用非归属网络的技巧。 |
| S0291 | 使用包括多种不同来源的研究方法来重建目标网络的技巧。 |
| S0292 | 熟练使用定位数据库和软件包。 |
| S0293 | 熟练使用工具，技术和程序来远程利用和建立目标上的持久性。 |
| S0294 | 熟练使用跟踪路线工具并解释结果，因为它们适用于网络分析和重建。 |
| S0295 | 熟练使用各种开源数据收集工具（网上交易，DNS，邮件等）。 |
| S0296 | 利用反馈改进流程，产品和服务的技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0297 | 利用虚拟协作工作空间和/或工具（例如，IWS，VTC，聊天室，SharePoint）方面的技能。 |
| S0298 | 熟练验证所有文件的完整性。 （例如，校验和，异或，安全散列，检查约束等）。 |
| S0299 | 无线网络目标分析，模板和地理位置技能。 |
| S0300 | 撰写（和提交）技能以满足技术能力方面的差距。 |
| S0301 | 以清晰，有说服力和有组织的方式写下关于事实和想法的技巧。 |
| S0302 | 撰写有效性报告的技巧。 |
| S0303 | 写作，审查和编辑来自多个来源的网络相关智能/评估产品的技能。 |
| S0304 | 获取当前可用资产信息的使用技巧。 |
| S0305 | 访问维护计划/指令/指导的数据库的技能。 |
| S0306 | 分析需要澄清和/或额外指导的问题的战略指导的技巧。 |
| S0307 | 分析目标或威胁来源的能力和精力的技能。 |
| S0308 | 预测情报能力就业要求的技能。 |
| S0309 | 预测可能促成领导决策的关键目标或威胁活动的技能。 |
| S0310 | 应用分析标准评估情报产品的技能。 |
| S0311 | 应用可用平台，传感器，架构和设备的功能，限制和任务方法，适用于组织目标的技能。 |
| S0312 | 应用用于评估网络操作性能和影响的过程的技能。 |
| S0313 | 表达需求声明/要求的技能，并将新的和新兴的采集能力，访问和/或过程集成到采集操作中。 |
| S0314 | 阐明可用于支持执行计划的情报能力的技能。 |
| S0315 | 能够向所有来源分析师阐明联合计划者的需求。 |
| S0316 | 将智力差距与优先信息需求和可观察量相关联的技能。 |
| S0317 | 比较指标/观察结果与要求的技能。 |
| S0318 | 概念化多个领域和维度中的整个知识过程的技能。 |
| S0319 | 将知识需求转化为知识生产任务的技能。 |
| S0320 | 协调量身定制的情报产品发展的技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0321 | 将情报优先级与情报资源/资产分配联系起来的技能。 |
| S0322 | 制定运营进展/成功的指标的技能。 |
| S0323 | 创建和维护最新的规划文件和跟踪服务/生产的技能。 |
| S0324 | 确定收集可行性的技巧。 |
| S0325 | 有能力制定收集计划，清楚地显示可用于收集所需信息的规范。 |
| S0326 | 区分名义资源和实际资源及其对正在开发的计划的适用性的技能。 |
| S0327 | 确保收集策略利用所有可用资源的技能。 |
| S0328 | 评估操作环境因素对目标和信息要求的技能。 |
| S0329 | 评估信息请求以确定是否存在响应信息的技能。 |
| S0330 | 评估有机，战区，国家，联盟和其他收集能力的能力，限制和任务方法的技能。 |
| S0331 | 能够口头和书面表达情报能力限制和决策风险与整体运作影响之间的关系。 |
| S0332 | 与收集要求和收集操作管理相关的可用工具和应用程序中提取信息的技能。 |
| S0333 | 以图形方式描述包含情报和合作伙伴能力估计的决策支持材料的技能。 |
| S0334 | 识别和应用任务，收集，处理，开发和传播到相关收集规范的技能。 |
| S0335 | 识别智力差距的技能。 |
| S0336 | 确定何时满足优先信息要求的技能。 |
| S0337 | 执行评估收集管理和操作活动的既定程序的技能。 |
| S0338 | 解释规划指导以辨别所需的分析支持水平的技能。 |
| S0339 | 掌握准备情况报告，运营相关性和情报收集影响的技巧。 |
| S0340 | 监测目标或威胁情况和环境因素的技能。 |
| S0341 | 监视对合作伙伴功能的威胁影响并保持运行估算的技能。 |
| S0342 | 通过反复调整，测试和重新调整来优化收集系统性能的技巧。 |
| S0343 | 协调情报规划团队，协调收集和生产支持以及监视状态。 |
| S0344 | 准备和交付报告，演示和简报的技巧，包括使用视觉辅助工具或演示技术。 |
| S0345 | 将情报资源/资产与预期的情报需求联系起来的技能。 |
| S0346 | 解决冲突的收集要求技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0347 | 审查关于收集资产的性能规范和历史信息的技能。 |
| S0348 | 指定必须在近期进行的收集和/或任务的技能。 |
| S0349 | 将操作评估程序与关键信息需求过程同步的技能。 |
| S0350 | 同步计划活动和所需的情报支持的技能。 |
| S0351 | 翻译有组织的，战区，国家，联盟和其他收集能力的能力，限制和任务方法的技能。 |
| S0352 | 使用协作工具和环境进行收集操作的技能。 |
| S0353 | 使用系统和/或工具跟踪收集要求并确定他们是否满意的技能。 |
| S0354 | 有能力制定反映企业核心隐私目标的政策。 |
| S0355 | 协商供应商协议和评估供应商隐私惯例的技能。 |
| S0356 | 熟练与包括董事会成员在内的所有管理层进行沟通（例如，人际交往技巧，可接近性，有效的倾听技巧，适合听众的风格和语言）。 |
| S0357 | 预测新的安全威胁技能。 |
| S0358 | 熟练掌握不断发展的技术基础设施。 |
| S0359 | 使用批判性思维分析组织模式和关系的技巧。 |
| S0360 | 分析和评估内部和外部合作伙伴网络运营能力和工具的技能。 |
| S0361 | 分析和评估内部和外部合作伙伴情报流程以及制定信息需求和重要信息的技能。 |
| S0362 | 分析和评估内部和外部合作伙伴组织的能力和局限性（具有任务，收集，处理，利用和传播责任的人员）的技能。 |
| S0363 | 分析和评估内部和外部合作伙伴报告的技能。 |
| S0364 | 熟练掌握组织威胁环境的背景知识 |
| S0365 | 设计云服务模型的事件响应技能。 |
| S0366 | 确定成功的能力，找到解决不太常见和更复杂的系统问题解决方案的技能。 |
| S0367 | 将网络安全和隐私原则应用于组织要求（与机密性，完整性，可用性，认证，不可否认性相关）的技能。 |
| S0368 | 使用风险评分来通知基于绩效和成本效益的方法，以帮助组织识别，评估和管理网络安全风险技能。 |

| 技能 ID | 描述 |
| --- | --- |
| S0369 | 识别组织数据资产的来源，特征和用途的技能。 |
| S0370 | 在自己的组织内部使用网络防务服务提供商报告结构和流程的技能。 |
| S0371 | 响应并采取当地行动来应对来自服务提供商的威胁共享警报的技能。 |
| S0372 | 翻译，追踪和优先考虑扩展企业中的信息需求和情报收集需求的技能。 |
| S0373 | 确保为信息系统和信息通信技术供应链基础设施组件收集问责制信息的技能。 |
| S0374 | 识别网络安全和隐私问题的技巧，这些问题源自与内部和外部客户以及合作伙伴组织的关系。 |

## A.7 NICE 框架能力描述

表 7 列出了网络安全能力。 能力是执行可观察行为或导致可观察产品的行为的能力。附录 B 列出了详细工作角色中的每个工作角色中列出的列表中选定的能力描述。此列表将定期更新[1]。 NIST 特别出版物 800-181 [4]的参考电子表格中可以找到该材料最新版本的权威来源。

**表 7 - NICE 框架能力描述**

| 能力 ID | 描述 |
| --- | --- |
| A0001 | 能够根据漏洞和配置数据的分析识别系统安全问题。 |
| A0002 | 能够针对给定应用程序或环境匹配适当的知识库技术。 |
| A0003 | 能够确定技术趋势数据的有效性。 |
| A0004 | 能够开发适合目标受众的恰当水平的课程。 |
| A0005 | 能够解密数字数据收集。 |
| A0006 | 能够准备和提供教育和意识简报，以确保系统，网络和数据用户了解并遵守系统安全策略和程序。 |
| A0007 | 能够为特定于应用程序的问题定制代码分析。 |

| 能力 ID | 描述 |
| --- | --- |
| A0008 | 能够应用这些方法，标准和描述，分析和记录组织的企业信息技术（IT）体系结构（例如，开放组架构框架[TOGAF]，国防部架构框架[DoDAF]，联邦企业架构框架[FEAF]）。 |
| A0009 | 能够应用供应链风险管理标准。 |
| A0010 | 分析恶意软件的能力。 |
| A0011 | 能够以清晰简洁的方式回答问题。 |
| A0012 | 有澄清问题的能力。 |
| A0013 | 能够通过口头，书面和/或视觉方式以自信和组织良好的方式传达复杂的信息，概念或想法。 |
| A0014 | 有效沟通的写作能力。 |
| A0015 | 能够进行漏洞扫描并识别安全系统中的漏洞。 |
| A0016 | 能够促进小组讨论。 |
| A0017 | 能够衡量学习者的理解和知识水平。 |
| A0018 | 准备和介绍简报的能力。 |
| A0019 | 能够生成技术文档。 |
| A0020 | 能够为学生提供有效的反馈以改善学习。 |
| A0021 | 能够使用和理解复杂的数学概念（例如离散数学）。 |
| A0022 | 能够应用成人学习的原则。 |
| A0023 | 能够设计有效和可靠的评估。 |
| A0024 | 能够制定明确的方向和教学材料。 |
| A0025 | 能够准确定义故障系统中的事故，问题和事件。 |
| A0026 | 分析测试数据的能力。 |
| A0027 | 能够应用组织的目标和目标来开发和维护架构。 |
| A0028 | 能够评估和预测满足组织目标的人力需求。 |
| A0029 | 能够构建复杂的数据结构和高级编程语言。 |
| A0030 | 能够收集，验证和验证测试数据。 |
| A0031 | 能够开展和实施市场调查，以了解政府和行业能力以及适当的定价。 |

| 能力 ID | 描述 |
| --- | --- |
| A0032 | 能够开发在虚拟环境中使用的课程。 |
| A0033 | 能够根据支持组织网络活动的法律，法规，政策和标准制定政策，计划和战略。 |
| A0034 | 能够开发，更新和/或维护标准操作程序（SOP）。 |
| A0035 | 能够剖析问题并检查可能不相关的数据之间的相互关系。 |
| A0036 | 能够高水平地识别基本的常见编码缺陷。 |
| A0037 | 能够利用有关网络问题的外部组织和学术机构的最佳实践和经验教训。 |
| A0038 | 能够优化系统以满足企业性能要求。 |
| A0039 | 能够监督生命周期成本估算的发展和更新。 |
| A0040 | 能够将数据和测试结果转化为评估结论。 |
| A0041 | 能够使用数据可视化工具（例如 Flare，HighCharts，AmCharts，D3.js，Processing，Google Visualization API，Tableau，Raphael.js）。 |
| A0042 | 有能力开发职业发展机会。 |
| A0043 | 能够在 Windows 和 Unix / Linux 环境中进行取证分析。 |
| A0044 | 能够应用编程语言结构（例如源代码审查）和逻辑。 |
| A0045 | 能够评估/确保供应商和/或产品的可信度。 |
| A0046 | 能够监控和评估新兴技术对法律，法规和/或政策的潜在影响。 |
| A0047 | 根据安全的软件部署方法，工具和实践开发安全软件的能力。 |
| A0048 | 能够应用网络安全体系结构概念，包括拓扑，协议，组件和原则（例如应用纵深防御）。 |
| A0049 | 能够应用安全的系统设计工具，方法和技术。 |
| A0050 | 能够应用系统设计工具，方法和技术，包括自动化系统分析和设计工具。 |
| A0051 | 能够执行技术集成流程。 |
| A0052 | 能够操作网络设备，包括集线器，路由器，交换机，网桥，服务器，传输介质和相关硬件。 |
| A0053 | 能够确定劳动力趋势数据的有效性。 |
| A0054 | 能够应用教学系统设计（ISD）方法。 |

| 能力 ID | 描述 |
| --- | --- |
| A0055 | 能够操作通用网络工具（例如 ping，traceroute，nslookup）。 |
| A0056 | 在整个采购过程中都能够确保安全实践的能力。 |
| A0057 | 能够针对目标受众制定适合于该主题的课程。 |
| A0058 | 能够执行 OS 命令行（例如，ipconfig，netstat，dir，nbtstat）。 |
| A0059 | 能够操作组织的 LAN / WAN 路径。 |
| A0060 | 能够构建体系结构和框架。 |
| A0061 | 能够设计架构和框架。 |
| A0062 | 能够监测措施或指标 |
| A0063 | 能够操作不同的电子通信系统和方法（例如，电子邮件，VOIP，IM，网络论坛，直接视频广播）。 |
| A0064 | 能够解读客户需求并将其转化为运营能力。 |
| A0065 | 能够监控网络中的流量。 |
| A0066 | 能够准确完整地获取智能，评估和/或计划产品中使用的所有数据。 |
| A0067 | 能够适应并在多元化，不可预知，具有挑战性和快节奏的工作环境中运作。 |
| A0068 | 能够应用批准的计划制定和人员配置流程。 |
| A0069 | 能够运用协作技巧和策略。 |
| A0070 | 能够运用批判性阅读/思考技能。 |
| A0071 | 能够将语言和文化专业知识应用于分析。 |
| A0072 | 能够清晰地将知识要求转化为完善的研究问题和数据跟踪变量，以便进行查询追踪。 |
| A0073 | 能够清晰地将知识要求转化为完善的研究问题和信息请求。 |
| A0074 | 与他人有效协作的能力。 |
| A0076 | 能够与分析人员就监视要求和重要信息开发进行协调和协作。 |
| A0077 | 能够协调网络运营与其他组织职能或支持活动。 |
| A0078 | 能够协调，协作和传播信息给下级，侧面和上级组织。 |
| A0079 | 能够将每个组织或元素正确运用到收集计划和矩阵中。 |

| 能力 ID | 描述 |
| --- | --- |
| A0080 | 能够针对信息不完整或无先例存在的问题和情况开发或推荐分析方法或解决方案。 |
| A0081 | 能够为没有先例存在的问题和情况制定或推荐计划解决方案。 |
| A0082 | 通过虚拟团队进行有效协作的能力。 |
| A0083 | 评估信息的可靠性，有效性和相关性的能力。 |
| A0084 | 能够评估，分析和综合大量数据（可能分散且矛盾）为高质量的融合目标/情报产品。 |
| A0085 | 当政策不明确时能够做出判断。 |
| A0086 | 通过开展目标分析和收集来确定感兴趣的目标，从而扩大网络访问的能力。 |
| A0087 | 能够集中研究工作来满足客户的决策需求。 |
| A0088 | 能够在动态，快节奏的环境中有效运作。 |
| A0089 | 能够在协作环境中发挥作用，不断寻求与组织内部和外部的其他分析师和专家的持续磋商，以利用分析和技术专业知识。 |
| A0090 | 能够识别具有共同网络操作兴趣的外部合作伙伴。 |
| A0091 | 能够识别情报差距。 |
| A0092 | 能够识别/描述目标漏洞。 |
| A0093 | 能够识别/描述对目标进行技术开发的技术/方法。 |
| A0094 | 能够解释和应用与组织网络目标相关的法律，法规，政策和指导。 |
| A0095 | 能够将客户需求理解并转化为操作行为。 |
| A0096 | 能够理解和理解复杂且快速发展的概念 |
| A0097 | 能够监控系统操作并响应触发事件对事件作出反应和/或观察趋势或异常活动。 |
| A0098 | 根据需要作为计划小组，协调小组和专责小组的成员参与。 |
| A0099 | 能够执行网络收集策略，技术和程序，包含解密功能/工具。 |
| A0100 | 能够执行无线收集程序，包含解密功能/工具。 |
| A0101 | 能够识别和缓解可能影响分析的认知偏差。 |
| A0102 | 能够识别和减轻报告和分析中的欺骗行为。 |
| A0103 | 能够审查处理后的目标语言材料的准确性和完整性。 |

| 能力 ID | 描述 |
| --- | --- |
| A0104 | 能够选择合适的注入来实现操作目标。 |
| A0105 | 能够根据客户的理解水平定制技术和计划信息。 |
| A0106 | 有批判性思考的能力。 |
| A0107 | 能够像构建威胁场景。 |
| A0108 | 能够理解目标和效果。 |
| A0109 | 能够在所有情报领域利用多种情报来源。 |
| A0110 | 能够监控信息隐私法律的更新，以确保组织的适应性和合规性。 |
| A0111 | 能够跨部门和业务部门工作，实施组织的隐私原则和计划，并将隐私目标与安全目标保持一致。 |
| A0112 | 能够监控信息隐私技术的进步，以确保组织的适应性和合规性。 |
| A0113 | 能够确定安全事件是否违反隐私原则或需要采取特定法律行动的法律标准。 |
| A0114 | 能够开发或采购适合目标的适当级别的课程。 |
| A0115 | 能够跨部门和业务部门工作，实施组织的隐私原则和计划，并将隐私目标与安全目标保持一致。 |
| A0116 | 能够正确有效地确定优先次序并分配网络安全资源。 |
| A0117 | 能够将组织动态背景下的战略，业务和技术联系起来。 |
| A0118 | 能够理解与组织过程和问题解决有关的技术，管理和领导问题。 |
| A0119 | 能够理解与网络及其组织影响相关的基本概念和问题。 |
| A0120 | 能够分享有关组织威胁环境背景的有意义的见解，从而改善其风险管理姿态。 |
| A0121 | 能够为云服务模型设计事件响应。 |
| A0122 | 能够设计功能来寻找解决不太常见和更复杂的系统问题的解决方案。 |
| A0123 | 能够将网络安全和隐私原则应用于组织需求（与机密性，完整性，可用性，身份验证和不可否认性相关）。 |
| A0124 | 能够建立和维护自动化安全控制评估 |
| A0125 | 根据现行法律撰写隐私披露声明的能力。 |
| A0126 | 能够跟踪跨部门，地点，设施的联网设备和软件的位置和配置，并可能支持业务功能。 |

| 能力 ID | 描述 |
| --- | --- |
| A0127 | 能够部署持续监控技术和工具。 |
| A0128 | 使用入侵检测技术应用技术检测主机和基于网络的入侵的能力。 |
| A0129 | 确保信息安全管理流程的能力与战略和运营规划流程相结合。 |
| A0130 | 能够确保组织内的高级官员为支持其控制下的运营和资产的信息和系统提供信息安全。 |
| A0131 | 能够确保组织拥有经过充分培训的人员来协助遵守立法，行政命令，政策，指令，指示，标准和指导方针中的安全要求。 |
| A0132 | 能够与组织的高级领导层进行协调，以提供全面的，全组织范围的整体方法来处理风险 – 这种方法可以更好地理解组织的整体运作。 |
| A0133 | 能够与组织的高层领导协调，为组织提供风险管理策略，为组织提供安全相关风险的战略视图。 |
| A0134 | 能够与组织的高层领导进行协调，以促进组织内授权官员和其他高级领导人之间共享风险相关信息。 |
| A0135 | 能够与组织的高层领导进行协调，以监督整个组织的所有风险管理相关活动，以帮助确保一致和有效的风险接受决策。 |
| A0136 | 能够与组织的高级领导层进行协调，以确保授权决定考虑到任务和业务成功所需的所有因素。 |
| A0137 | 能够与组织高级领导层进行协调，提供一个组织范围的论坛，以考虑组织运营和资产，个人，其他组织和国家的所有风险源（包括综合风险）。 |
| A0138 | 能够与组织的高层领导协调，促进授权官员之间的合作与协作，包括需要分担责任的授权行动。 |
| A0139 | 能够与组织的高级领导层进行协调，以确保使用系统，服务和应用程序的外部提供者支持组织任务/业务职能的共同责任获得所需的可见性，并提升给适当的决策机构。 |
| A0140 | 能够与组织高级领导层协调，根据组织负责的系统的运行和使用的总体风险来确定组织风险状况。 |

| 能力 ID | 描述 |
| --- | --- |
| A0141 | 能够与授权官员及其指定代表密切合作，帮助确保组织范围的安全计划得到有效实施，从而为所有组织系统和运营环境提供足够的安全保障。 |
| A0142 | 能够与授权官员及其指定代表密切合作，帮助确保安全考虑融入编程/计划/预算周期，企业架构以及采集/系统开发生命周期。 |
| A0143 | 能够与授权官员及其指定代表密切合作，帮助确保组织系统和共同控制措施被批准的安全计划涵盖并拥有最新的授权。 |
| A0144 | 能够与授权官员及其指定代表密切合作，帮助确保整个组织所需的与安全相关的活动以高效，经济高效和及时的方式完成。 |
| A0145 | 能够与授权官员及其指定代表密切合作，以确保集中报告与安全有关的活动。 |
| A0146 | 能够建立合适使用和保护信息的规则，并保留责任，即使信息与其他组织分享或提供给其他组织。 |
| A0147 | 能够批准安全计划，协议或理解备忘录，行动计划和里程碑，并确定系统或操作环境中的重大变化是否需要重新授权。 |
| A0148 | 能够担任企业架构师和系统安全工程师之间的主要联络员，并与系统所有者，公共控制提供者和系统安全官员协调安全控制的分配，如系统专用，混合或通用控制。 |
| A0149 | 能力与系统安全人员密切协调，就一系列与安全有关的问题（如建立系统）向授权官员，首席信息官，高级信息安全官员和风险管理/风险执行（职能）高级问责官员提供建议界限;评估系统弱点和缺陷的严重程度;行动计划和里程碑;风险缓解方法;安全警报;以及已识别漏洞的潜在不利影响）。 |
| A0150 | 能够开展系统安全工程活动（NIST SP 800-16）。 |
| A0151 | 通过有针对性的安全架构，设计，开发和配置，可以捕获和优化安全需求并确保需求有效地集成到组件产品和系统中。 |
| A0152 | 在包括软件工程方法在内的系统中实施安全控制时，能够采用最佳实践;系统和安全工程原理;安全设计，安全架构和安全编码技术。 |
| A0153 | 能够与安全架构师，高级信息安全官员，系统所有者，通用控制提供者和系统安全官员协调他们的安全相关活动。 |

| 能力 ID | 描述 |
| --- | --- |
| A0154 | 能够对系统中使用或继承的管理，操作和技术安全控制和增强控制进行综合评估，以确定控制的有效性（即，安全控制的实施程度是否正确，是否按预期运行并且在满足系统安全要求方面产生期望的结果）。 |
| A0155 | 能够评估系统及其运行环境中发现的弱点或缺陷的严重程度，并提出纠正措施以解决已识别的漏洞。 |
| A0156 | 能够编制包含评估结果和调查结果的最终安全评估报告。 |
| A0157 | 评估安全计划的能力，以帮助确保该计划为系统提供一组符合规定安全要求的安全控制。 |
| A0158 | 能够确保合同中适当处理功能和安全要求，并确保承包商符合合同中所述的功能和安全要求。 |
| A0159 | 能够解释由网络工具收集的信息（例如 Nslookup，Ping 和 Traceroute）。 |
| A0160 | 能够翻译，追踪和优先考虑扩展企业中的信息需求和情报收集需求。 |
| A0161 | 能够将信息安全要求整合到采购过程中;使用适用的基准安全控制作为安全要求的来源之一;确保强大的软件质量控制流程;并建立多个来源（例如，关键系统要素的运送路线）。 |
| A0162 | 能够确保信息系统安全，采购人员，法律顾问以及其他适当的顾问和利益相关者参与系统概念定义/评审的决策，并参与或批准系统整个系统生命周期中的每个里程碑决策。 |
| A0162 | 能够识别通信安全（COMSEC）环境和层次结构的独特方面。 |
| A0163 | 能够解释通信安全（COMSEC）术语，指导方针和程序。 |
| A0164 | 能够确定指定的通信安全（COMSEC）人员的角色和责任。 |
| A0165 | 能够管理通信安全（COMSEC）材料报告，控制和使用程序。 |
| A0166 | 能够识别通信安全（COMSEC）事件的类型及其报告方式 |
| A0167 | 能够认识到审计通信安全（COMSEC）材料和账户的重要性。 |
| A0168 | 能够识别通信安全（COMSEC）进程中的报告要求 |
| A0170 | 能够识别关键基础设施系统没有使用系统安全考虑因素设计的信息通信技术。 |
| A0171 | 能够进行培训和教育需求评估。 |

| 能力 ID | 描述 |
|---|---|
| A0172 | 能够建立将内部局域网（LAN）与其他不可信网络分开的物理或逻辑子网。 |
| A0173 | 能够认识到系统或环境的变化可以通过风险偏好改变相关的剩余风险。 |
| A0174 | 能够使用 TOR 网络查找和浏览暗网以查找市场和论坛。 |
| A0175 | 能够在多个操作系统平台上检查数字媒体。 |
| A0176 | 维护数据库的能力。（备份，恢复，删除数据，事务日志文件等）。 |

# 附录 B – 工作角色明细清单

本附录提供了每个 NICE 框架工作角色的详细说明。 对于每个工作角色，下面的列表提供了以下信息：

- 工作角色名称;
- 特有的 NICE 框架工作角色 ID，基于该工作角色所属的 NICE 框架类别和专业领域的缩写;
- 工作角色所在的专业领域;
- 工作角色所在的类别;
- 工作角色的描述;
- NICE 框架任务列表，包括工作角色的网络安全职位人员可能会执行;
- NICE 框架知识领域的列表，包括工作角色的网络安全职位的人员可能会展示;
- NICE 框架技能列表，包括工作角色的网络安全职位人员可能会拥有; 和
- NICE 框架能力列表，包括工作角色的网络安全职位的人员可能会被证明。

下表通过简单的任务，知识，技能和能力列表描述了 NICE 框架的工作角色。 NIST 特别出版物 800-181[4]的参考电子表格中可以找到该材料最新版本的权威来源。 参考电子表格提供了更详细的任务，知识，技能和能力列表。工作角色将定期更新[1]。

## B.1 安全准备（SP）

| 工作角色名称 | 授权官 |
|---|---|

| | |
|---|---|
| 工作角色 ID | SP-RSK-001 |
| 专业领域 | 风险管理（RSK） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 高级官员或执行官，有权正式承担在组织运营（包括任务，职能，形象或声誉），组织资产，个人，其他组织和国家可接受的风险水平下运营信息系统的责任（CNSSI4009）。 |
| 任务 | T0145, T0221, T0371, T0495 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624 |
| 技能 | S0034, S0367 |
| 能力 | A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170 |

| | |
|---|---|
| 工作角色名称 | 安全控制评估师 |
| 工作角色 ID | SP-RSK-002 |
| 专业领域 | 风险管理（RSK） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 对信息技术（IT）系统采用或继承的管理，运营和技术安全控制和控制增强进行独立综合评估，以确定控制的整体有效性（如 NIST 800-37 中所定义）。 |
| 任务 | T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, |

| | |
|---|---|
| | K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624 |
| 技能 | S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374 |
| 能力 | A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170 |

| | |
|---|---|
| 工作角色名称 | 软件开发 |
| 工作角色 ID | SP-DEV-001 |
| 专业领域 | 软件开发（DEV） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 开发，创建，维护和编写/编码新的（或修改现有的）计算机应用程序，软件或专用实用程序。 |
| 任务 | T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, |

| | |
|---|---|
| | K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624 |
| 技能 | S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367 |
| 能力 | A0007, A0021, A0047, A0123, A0170 |

| | |
|---|---|
| 工作角色名称 | 安全软件评估 |
| 工作角色 ID | SP-DEV-002 |
| 专业领域 | 软件开发（DEV） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 分析新的或现有的计算机应用程序，软件或专用实用程序的安全性并提供可操作的结果。 |
| 任务 | T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624 |
| 技能 | S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367 |
| 能力 | A0021, A0123, A0170 |

| | |
|---|---|
| 工作角色名称 | 企业架构师 |
| 工作角色 ID | SP-ARC-001 |
| 专业领域 | 系统架构（ARC） |
| 类别 | 安全准备（SP） |

| | |
|---|---|
| 工作角色描述 | 开发并维护业务，系统和信息流程以支持企业任务需求；开发描述基线和目标体系结构的信息技术（IT）规则和要求。 |
| 任务 | T0051，T0084，T0090，T0108，T0196，T0205，T0307，T0314，T0328，T0338，T0427，T0440，T0448，T0473，T0517，T0521，T0542，T0555，T0557 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0024，K0027，K0028，K0030，K0035，K0037，K0043，K0044，K0052，K0056，K0060，K0061，K0063，K0074，K0075，K0082，K0091，K0093，K0102，K0170，K0179，K0180，K0198，K0200，K0203，K0207，K0211，K0212，K0214，K0227，K0240，K0264，K0275，K0286，K0287，K0291，K0293，K0299，K0322，K0323，K0325，K0326，K0332，K0333，K0487，K0516 |
| 技能 | S0005，S0024，S0027，S0050，S0060，S0122，S0367，S0374 |
| 能力 | A0008，A0015，A0027，A0038，A0051，A0060，A0123，A0170 |

| | |
|---|---|
| 工作角色名称 | 安全架构 |
| 工作角色 ID | SP-ARC-002 |
| 专业领域 | 系统架构（ARC） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 确保在企业架构的所有方面（包括参考模型，细分市场和解决方案架构以及支持这些任务和业务流程的最终系统）充分解决保护组织的使命和业务流程所需的利益相关方安全需求。 |
| 任务 | T0050，T0051，T0071，T0082，T0084，T0090，T0108，T0177，T0196，T0203，T0205，T0268，T0307，T0314，T0328，T0338，T0427，T0448，T0473，T0484，T0542，T0556 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0007，K0008，K0009，K0010，K0011，K0012，K0013，K0015，K0018，K0019，K0024，K0026，K0027，K0030，K0035，K0036，K0037，K0043，K0044，K0052，K0055，K0056，K0057，K0059，K0060，K0061，K0063，K0071，K0074，K0082，K0091，K0092，K0093，K0102，K0170，K0180，K0198，K0200，K0202， |

| | |
|---|---|
| | K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0374, K0565 |
| 技能 | S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374 |
| 能力 | A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172 |

| | |
|---|---|
| 工作角色名称 | 研究和开发专家 |
| 工作角色 ID | SP-TRD-001 |
| 专业领域 | 技术研发（TRD） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 开展软件和系统工程和软件系统研究，开发新功能，确保网络安全完全整合。 开展全面的技术研究，以评估网络空间系统的潜在脆弱性。 |
| 任务 | T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499 |
| 技能 | S0005, S0017, S0072, S0140, S0148, S0172 |
| 能力 | A0001, A0018, A0019, A0170 |

| | |
|---|---|
| 工作角色名称 | 系统需求规划员 |
| 工作角色 ID | SP-SRP-001 |
| 专业领域 | 系统需求规划（SRP） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 咨询客户以评估功能需求并将功能需求转化为技术解决方案。 |
| 任务 | T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, |

| | |
|---|---|
| | T0463, T0497 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622 |
| 技能 | S0005, S0006, S0008, S0010, S0050, S0134, S0367 |
| 能力 | A0064, A0123, A0170 |

| | |
|---|---|
| 工作角色名称 | 系统测试和评估专家 |
| 工作角色 ID | SP-TST-001 |
| 专业领域 | 测试和评估（TST） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 计划，准备并执行系统测试，根据规格和要求评估结果，并分析/报告测试结果。 |
| 任务 | T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332 |
| 技能 | S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367 |
| 能力 | A0026, A0030, A0040, A0123 |

| | |
|---|---|
| 工作角色名称 | 信息系统安全开发者 |
| 工作角色 ID | SP-SYS-001 |
| 专业领域 | 系统开发（SYS） |
| 类别 | 安全准备（SP） |

| | |
|---|---|
| 工作角色描述 | 在整个系统开发生命周期中设计，开发，测试和评估信息系统安全。 |
| 任务 | T0012，T0015，T0018，T0019，T0021，T0032，T0053，T0055，T0056，T0061，T0069，T0070，T0076，T0078，T0105，T0107，T0109，T0119，T0122，T0124，T0181，T0201，T0205，T0228，T0231，T0242，T0269，T0270，T0271，T0272，T0304，T0326，T0359，T0446，T0449，T0466，T0509，T0518，T0527，T0541，T0544 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0015，K0018，K0024，K0027，K0028，K0030，K0032，K0035，K0036，K0044，K0045，K0049，K0050，K0052，K0055，K0056，K0060，K0061，K0063，K0065，K0066，K0067，K0073，K0081，K0082，K0084，K0086，K0087，K0090，K0091，K0093，K0102，K0126，K0139，K0169，K0170，K0179，K0180，K0200，K0203，K0260，K0261，K0262，K0276，K0287，K0297，K0308，K0322，K0325，K0332，K0333，K0336 |
| 技能 | S0001，S0022，S0023，S0024，S0031，S0034，S0036，S0085，S0145，S0160，S0367 |
| 能力 | A0001，A0008，A0012，A0013，A0015，A0019，A0026，A0040，A0048，A0049，A0050，A0056，A0061，A0074，A0089，A0098，A0108，A0119，A0123，A0170 |

| | |
|---|---|
| 工作角色名称 | 系统开发者 |
| 工作角色 ID | SP-SYS-002 |
| 专业领域 | 系统开发（SYS） |
| 类别 | 安全准备（SP） |
| 工作角色描述 | 在整个系统开发生命周期中设计，开发，测试和评估信息系统。 |
| 任务 | T0012，T0021，T0053，T0056，T0061，T0067，T0070，T0107，T0109，T0119，T0181，T0201，T0205，T0228，T0242，T0304， |

| | |
|---|---|
| | T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336 |
| 技能 | S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367 |
| 能力 | A0123, A0170 |

## B.2 操作和维护（OM）

| | |
|---|---|
| 工作角色名称 | 数据库管理员 |
| 工作角色 ID | OM-DTA-001 |
| 专业领域 | 数据管理员（DTAA） |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 管理允许安全存储，查询和使用数据的数据库和/或数据管理系统。 |
| 任务 | T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420 |
| 技能 | S0002, S0013, S0037, S0042, S0045 |

| | |
|---|---|
| 能力 | A0176 |

| | |
|---|---|
| 工作角色名称 | 数据分析 |
| 工作角色 ID | OM-DTA-002 |
| 专业领域 | 数据管理员（DTA） |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 检查来自多个不同来源的数据，以提供安全和隐私洞察。 设计和实施用于建模，数据挖掘和研究目的的复杂企业级数据集的自定义算法，工作流程和布局。 |
| 任务 | T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420 |
| 技能 | S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369 |
| 能力 | A0029, A0035, A0036, A0041, A0066 |

| | |
|---|---|
| 工作角色名称 | 知识经理 |
| 工作角色 ID | OM-KMG-001 |
| 专业领域 | 知识管理（KMG） |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 描述负责管理和流程和工具管理，使组织能够识别，记录和访问知识资本和信息内容。 |
| 任务 | T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524 |

| | |
|---|---|
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420 |
| 技能 | S0011, S0012, S0049, S0055 |
| 能力 | A0002 |

| | |
|---|---|
| 工作角色名称 | 技术支持专家 |
| 工作角色 ID | OM-STS-001 |
| 专业领域 | 客户服务和技术支持 (STS) |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 根据已建立或已批准的组织流程组件，为需要使用客户端级硬件和软件的客户提供技术支持。(即适用的主事件管理计划)。 |
| 任务 | T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330 |
| 技能 | S0039, S0058, S0142, S0159, S0365 |
| 能力 | A0025, A0034, A0122 |

| | |
|---|---|
| 工作角色名称 | 网络运营专家 |
| 工作角色 ID | OM-NET-001 |
| 专业领域 | 网络服务（NET） |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 计划，实施和运营网络服务/系统，包括硬件和虚拟环境。 |
| 任务 | T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, |

| | |
|---|---|
| | K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622 |
| 技能 | S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170 |
| 能力 | A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159 |

| | |
|---|---|
| 工作角色名称 | 系统管理员 |
| 工作角色 ID | OM-ADM-001 |
| 专业领域 | 系统管理（ADM） |
| 类别 | 操作和维护（OM） |
| 工作角色描述 | 负责设置和维护系统或系统的特定组件（例如，安装，配置和更新硬件和软件;建立和管理用户帐户;监督或执行备份和恢复任务;实施操作和技术安全控制; 并遵守组织安全政策和程序）。 |
| 任务 | T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346 |
| 技能 | S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158 |
| 能力 | A0025, A0027, A0034, A0055, A0062, A0074, A0088, A0123, A0124 |

| | |
|---|---|
| 工作角色名称 | 系统安全分析师 |
| 工作角色 ID | OM-ANA-001 |
| 专业领域 | 系统分析（ANA） |
| 类别 | 操作和维护（OM） |

| | |
|---|---|
| 工作角色描述 | 负责分析和开发系统安全的集成，测试，操作和维护。 |
| 任务 | T0015，T0016，T0017，T0085，T0086，T0088，T0123，T0128，T0169，T0177，T0187，T0194，T0202，T0205，T0243，T0309，T0344，T0462，T0469，T0470，T0475，T0477，T0485，T0489，T0492，T0499，T0504，T0508，T0526，T0545，T0548 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0015，K0018，K0019，K0024，K0035，K0036，K0040，K0044，K0049，K0052，K0056，K0060，K0061，K0063，K0075，K0082，K0093，K0102，K0179，K0180，K0200，K0203，K0227，K0260，K0261，K0262，K0263，K0266，K0267，K0275，K0276，K0281，K0284，K0285，K0287，K0290，K0297，K0322，K0333，K0339 |
| 技能 | S0024，S0027，S0031，S0036，S0060，S0141，S0147，S0167，S0367 |
| 能力 | A0015，A0123 |

## B.3 监督和治理（OV）

| | |
|---|---|
| 工作角色名称 | 网络法律顾问 |
| 工作角色 ID | OV-LGA-001 |
| 专业领域 | 法律咨询和倡导（LGA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 就网络法相关主题提供法律咨询和建议。 |
| 任务 | T0006，T0098，T0102，T0131，T0220，T0419，T0434，T0465，T0474，T0476，T0478，T0487，T0522 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0017，K0059，K0107，K0157，K0261，K0262，K0267，K0312，K0316，K0341，K0615 |
| 技能 | S0356 |
| 能力 | A0046 |

| | |
|---|---|
| 工作角色名称 | 隐私官/隐私合规经理 |
| 工作角色 ID | OV-LGA-002 |
| 专业领域 | 法律咨询和倡导（LGA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 开发和监督隐私合规计划和隐私计划人员，支持隐私和安全管理人员及其团队的隐私合规性，治理/政策和事件响应需求。 |
| 任务 | T0003，T0004，T0029，T0930，T0032，T0066，T0098，T0099，T0131，T0133，T0188，T0381，T0384，T0478，T0861，T0862，T0863，T0864，T0865，T0866，T0867，T0868，T0869，T0870，T0871，T0872，T0873，T0874，T0875，T0876，T0877，T0878，T0879，T0880，T0881，T0882，T0883，T0884，T0885，T0886，T0887，T0888，T0889，T0890，T0891，T0892，T0893，T0894，T0895，T0896，T0897，T0898，T0899，T0900，T0901，T0902，T0903，T0904，T0905，T0906，T0907，T0908，T0909，T0910，T0911，T0912，T0913，T0914，T0915，T0916，T0917，T0918，T0919 |
| 知识 | K0001，K0002，K0003，K0004，K0005，K0006，K0008，K0066，K0168，K0612，K0613，K0614，K0615 |
| 技能 | S0354，S0355，S0356 |
| 能力 | A0024，A0033，A0034，A0104，A0105，A0110，A0111，A0112，A0113，A0114，A0115，A0125 |

| | |
|---|---|
| 工作角色名称 | 网络教育课程开发者 |
| 工作角色 ID | OV-TEA-001 |
| 专业领域 | 培训，教育和意识（TEA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 说明根据教学需求开发，计划，协调和评估网络培训/教育课程，方法和技术。 |
| 任务 | T0230，T0247，T0248，T0249，T0345，T0352，T0357，T0365， |

| | |
|---|---|
| | T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628 |
| 技能 | S0064, S0066, S0070, S0102, S0166, S0296 |
| 能力 | A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171 |

| | |
|---|---|
| 工作角色名称 | 网络教师 |
| 工作角色 ID | OV-TEA-002 |
| 专业领域 | 培训，教育和意识（TEA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 开发并开展网络领域内人员的培训或教育。 |
| 任务 | T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628 |
| 技能 | S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358 |
| 能力 | A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, |

| | |
|---|---|
| | A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171 |

| | |
|---|---|
| 工作角色名称 | 信息系统安全经理 |
| 工作角色 ID | OV-MGT-001 |
| 专业领域 | 网络安全管理（MGT） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 负责项目，组织，系统或飞地的网络安全。 |
| 任务 | T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624 |
| 技能 | S0018, S0027, S0086 |
| 能力 | A0128, A0161, A0170 |

| | |
|---|---|
| 工作角色名称 | 通信安全（COMSEC）经理 |
| 工作角色 ID | OV-MGT-002 |
| 专业领域 | 网络安全管理（MGT） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 管理组织通信安全（COMSEC）资源的个人（CNSSI 4009）或加密密 |

| | |
|---|---|
| | 钥管理系统（CKMS）的密钥管理员。 |
| 任务 | T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622 |
| 技能 | S0027, S0059, S0138 |
| 能力 | A0162, A0163, A0164, A0165, A0166, A0167, A0168 |

| | |
|---|---|
| 工作角色名称 | 网络劳动力开发人员和经理 |
| 工作角色 ID | OV-SPP-001 |
| 专业领域 | 战略规划与政策（SPP） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 制定网络空间劳动力计划，战略和指导，以支持网络空间劳动力的人力，人员，培训和教育需求，并解决网络空间政策，原则，物资，队伍结构以及教育和培训要求的变化。 |
| 任务 | T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335 |
| 技能 | S0108, S0128 |
| 能力 | A0023, A0028, A0033, A0037, A0042, A0053 |

| | |
|---|---|
| 工作角色名称 | 网络政策和策略规划 |
| 工作角色 ID | OV-SPP-002 |

| | |
|---|---|
| 专业领域 | 战略规划和政策发展（SPP） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 制定和维护网络安全计划，战略和政策，以支持并符合组织网络安全举措和法规遵从。 |
| 任务 | T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624 |
| 技能 | S0176, S0250 |
| 能力 | A0003, A0033, A0037 |

| | |
|---|---|
| 工作角色名称 | 行政网络领导 |
| 工作角色 ID | OV-EXL-001 |
| 专业领域 | 行政网络领导力（EXL） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 执行决策权并为组织的网络和网络相关资源和/或运营确定愿景和方向。 |
| 任务 | T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628 |
| 技能 | S0018, S0356, S0357, S0358, S0359 |
| 能力 | A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130 |

| | |
|---|---|
| 工作角色名称 | 项目经理 |

| | |
|---|---|
| 工作角色 ID | OV-PMA-001 |
| 专业领域 | 计划/项目管理和采购（PMA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 领导，协调，沟通，整合，并对项目的整体成功负责，确保与机构或企业优先事项保持一致。 |
| 任务 | T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270 |
| 技能 | S0038, S0372 |
| 能力 | A0009, A0039, A0045, A0056 |

| | |
|---|---|
| 工作角色名称 | 信息技术（IT）项目经理 |
| 工作角色 ID | OV-PMA-002 |
| 专业领域 | 计划/项目管理和采购（PMA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 直接管理信息技术项目。 |
| 任务 | T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270 |
| 技能 | S0038, S0372 |

| | |
|---|---|
| 能力 | A0009, A0039, A0045, A0056 |

| | |
|---|---|
| 工作角色名称 | 产品支持经理 |
| 工作角色 ID | OV-PMA-003 |
| 专业领域 | 计划/项目管理和采购（PMA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 管理现场所需的一系列支持功能，并保持系统和组件的准备就绪和运营能力。 |
| 任务 | T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270 |
| 技能 | S0038, S0372 |
| 能力 | A0009, A0031, A0039, A0045, A0056 |

| | |
|---|---|
| 工作角色名称 | IT 投资/投资组合经理 |
| 工作角色 ID | OV-PMA-004 |
| 专业领域 | 计划/项目管理和采购（PMA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 管理符合特派团和企业优先事项总体需求的 IT 投资组合。 |
| 任务 | T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270 |
| 技能 | S0372 |
| 能力 | A0039 |

| | |
|---|---|
| 工作角色名称 | IT 计划审计员 |
| 工作角色 ID | OV-PMA-005 |
| 专业领域 | 计划/项目管理和采购（PMA） |
| 类别 | 监督和治理（OV） |
| 工作角色描述 | 对 IT 计划或其各个组件进行评估，以确定是否符合公布的标准。 |
| 任务 | T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270 |
| 技能 | S0038, S0085, S0372 |
| 能力 | A0056 |

## B.4 保护和防御（PR）

| | |
|---|---|
| 工作角色名称 | 网络防御分析师 |
| 工作角色 ID | PR-CDA-001 |
| 专业领域 | 网络防御分析（CDA） |
| 类别 | 保护和防御（PR） |
| 工作角色描述 | 使用从各种网络防御工具（例如，IDS 警报，防火墙，网络流量日志）收集的数据来分析其环境中发生的事件，以减轻威胁。 |
| 任务 | T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, |

| | |
|---|---|
| | K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624 |
| 技能 | S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370 |
| 能力 | A0010, A0015, A0066, A0123, A0128, A0159 |

| | |
|---|---|
| 工作角色名称 | 网络防御基础架构支持专家 |
| 工作角色 ID | PR-INF-001 |
| 专业领域 | 网络防御基础设施支持（INF） |
| 类别 | 保护和防御（PR） |
| 工作角色描述 | 测试，实施，部署，维护和管理基础架构硬件和软件。 |
| 任务 | T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058. K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332,K0334 |
| 技能 | S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367 |
| 能力 | A0123 |

| | |
|---|---|
| 工作角色名称 | 网络防御事件响应人员 |
| 工作角色 ID | PR-CIR-001 |
| 专业领域 | 事件响应（CIR） |
| 类别 | 保护和防御（PR） |
| 工作角色描述 | 调查，分析并回应网络环境或飞地内的网络事件。 |
| 任务 | T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, |

| | |
|---|---|
| | T0510 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624 |
| 技能 | S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365 |
| 能力 | A0121, A0128 |

| | |
|---|---|
| 工作角色名称 | 漏洞评估分析师 |
| 工作角色 ID | PR-VAM-001 |
| 专业领域 | 漏洞评估和管理（VAM） |
| 类别 | 保护和防御（PR） |
| 工作角色描述 | 对网元或飞地内的系统和网络进行评估，并确定这些系统/网络是否偏离可接受配置，飞地策略或本地策略的位置。 测量深度防御架构针对已知漏洞的有效性。 |
| 任务 | T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624 |
| 技能 | S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367 |
| 能力 | A0001, A0044, A0120, A0123 |

## B.5 分析（AN）

| | |
|---|---|
| 工作角色名称 | 威胁/警告分析师 |
| 工作角色 ID | AN-TWA-001 |
| 专业领域 | 警告/威胁分析（TWA） |

| | |
|---|---|
| 类别 | 分析（AN） |
| 工作角色描述 | 开发网络指标以保持对高度动态运行环境状态的认识。 收集，处理，分析和传播网络威胁/警告评估。 |
| 任务 | T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614 |
| 技能 | S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303 |
| 能力 | A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109 |

| | |
|---|---|
| 工作角色名称 | 开发分析师 |
| 工作角色 ID | AN-EXP-001 |
| 专业领域 | 开发分析（EXP） |
| 类别 | 分析（AN） |
| 工作角色描述 | 合作确定通过网络收集和/或准备活动可以满足的访问和收集满意程度。利用所有授权资源和分析技术来渗透目标网络。 |
| 任务 | T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, |

| | |
|---|---|
| | K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608 |
| 技能 | S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300 |
| 能力 | A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104 |

| | |
|---|---|
| 工作角色名称 | 全源分析师 |
| 工作角色 ID | AN-ASA-001 |
| 专业领域 | 全源分析（ASA） |
| 类别 | 分析（AN） |
| 工作角色描述 | 分析来自一个或多个来源的数据/信息，以开展环境准备，回应信息请求，并提交情报收集和生产要求以支持规划和运营。 |
| 任务 | T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0362, K0444, K0471, K0560, K0377, K0392, K0395, K0405, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0480, K0511, K0516, K0556, K0561, K0565, K0603, K0604, K0610, K0612, K0614, K0357, K0410, K0457, K0465, K0507, K0533, K0542, K0549, K0551, K0577, K0598 |

| | |
|---|---|
| 技能 | S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360 |
| 能力 | A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109 |

| | |
|---|---|
| 工作角色名称 | 任务评估专家 |
| 工作角色 ID | AN-ASA-002 |
| 专业领域 | 全源分析（ASA） |
| 类别 | 分析（AN） |
| 工作角色描述 | 制定评估计划和绩效/有效性措施。 根据网络活动的要求进行战略和运营效果评估。 确定系统是否按预期执行，并为确定运营有效性提供输入。 |
| 任务 | T0582, T0583, T0585, T0586, T0588, T0589, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614 |
| 技能 | S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360 |

| | |
|---|---|
| 能力 | A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108 |

| | |
|---|---|
| 工作角色名称 | 目标开发者 |
| 工作角色 ID | AN-TGT-001 |
| 专业领域 | 目标（TGT） |
| 类别 | 分析（AN） |
| 工作角色描述 | 执行目标系统分析，构建和/或维护电子目标文件夹，以包括来自环境准备和/或内部或外部情报源的输入。 与合作伙伴目标活动和情报组织协调，并提出候选目标进行审查和验证。 |
| 任务 | T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0142, K0349, K0362, K0444, K0471, K0560, K0392, K0395, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0460, K0464, K0516, K0556, K0561, K0565, K0603, K0604, K0614, K0457, K0465, K0507, K0549, K0551, K0598, K0417, K0458, K0357, K0533, K0542, K0351, K0379, K0473, K0381, K0402, K0413, K0426, K0439, K0461, K0466, K0478, K0479, K0497, K0499, K0543, K0546, K0547, K0555 |
| 技能 | S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361 |

| | |
|---|---|
| 能力 | A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073 |

| | |
|---|---|
| 工作角色名称 | 目标网络分析师 |
| 工作角色 ID | AN-TGT-002 |
| 专业领域 | 目标（TGT） |
| 类别 | 分析（AN） |
| 工作角色描述 | 对收集和开源数据进行高级分析，以确保目标的连续性；分析目标及其活动；并开发获取更多目标信息的技术。 根据对目标技术，数字网络及其应用的了解，确定目标如何进行通信，移动，操作和生活。 |
| 任务 | T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600 |
| 技能 | S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301 |
| 能力 | A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073 |

| | |
|---|---|
| 工作角色名称 | 多学科语言分析师 |
| 工作角色 ID | AN-LNG-001 |

| | |
|---|---|
| 专业领域 | 语言分析（LNG） |
| 类别 | 分析（AN） |
| 工作角色描述 | 应用具有目标/威胁和技术知识的语言和文化专业知识来处理，分析和/或传播从语言，语音和/或图形资料中获取的情报信息。 创建并维护特定于语言的数据库和工作辅助工具，以支持网络行动执行并确保关键知识共享。 提供外语密集或跨学科项目的主题专业知识。 |
| 任务 | T0650, T0606, T0715, T0745, T0761, T0837, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, T0860 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607 |
| 技能 | S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284 |
| 能力 | A0013, A0089, A0071, A0103 |

## B.6 收集和操作（CO）

| | |
|---|---|
| 工作角色名称 | 全源收集经理 |
| 工作角色 ID | CO-CLO-001 |
| 专业领域 | 收集操作（CLO） |
| 类别 | 收集和操作（CO） |
| 工作角色描述 | 确定收集行政管理和环境； 将优先信息要求纳入收集管理； 开发 |

| | |
|---|---|
| | 符合领导意图的概念。 确定可用收集资产的能力，确定新的收集能力；并构建和传播收集计划。 监控任务收集的执行情况，以确保收集计划的有效执行。 |
| 任务 | T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613 |
| 技能 | S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362 |
| 能力 | A0069, A0070, A0076, A0078, A0079 |

| | |
|---|---|
| 工作角色名称 | 全源收集需求管理者 |
| 工作角色 ID | CO-CLO-002 |
| 专业领域 | 收集操作（CLO） |
| 类别 | 收集和操作（CO） |

| | |
|---|---|
| 工作角色描述 | 评估收集操作并使用可用来源和方法开发基于收集需求策略效果来改进收集。 开发，处理，验证和协调收集要求的提交。 评估收集资产和收集操作的性能。 |
| 任务 | T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612 |
| 技能 | S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362 |
| 能力 | A0069, A0070, A0078 |

| | |
|---|---|
| 工作角色名称 | 网络国际规划 |
| 工作角色 ID | CO-OPL-001 |
| 专业领域 | 网络运营计划（OPL） |
| 类别 | 收集和操作（CO） |
| 工作角色描述 | 制定详细的情报计划以满足网络作战要求。 与网络运营规划人员合作确定，验证和征收收集和分析要求。 参与网络行动的选择， |

| | |
|---|---|
| | 验证，同步和执行。 同步情报活动以支持网络空间中的组织目标。 |
| 任务 | T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602 |
| 技能 | S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350, S0360 |
| 能力 | A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160 |

| | |
|---|---|
| 工作角色名称 | 网络运营计划 |

| | |
|---|---|
| 工作角色 ID | CO-OPL-002 |
| 专业领域 | 网络运营计划（OPL） |
| 类别 | 收集和操作（CO） |
| 工作角色描述 | 通过与其他计划者，运营商和/或分析师的合作，制定详细的计划，以管理或支持适用范围的网络运营。参与定位选择，验证，同步，并使得网络操作的执行过程中的整合。 |
| 任务 | T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565 K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614 |
| 技能 | S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360 |
| 能力 | A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105 |

| | |
|---|---|
| 工作角色名称 | 合作伙伴集成规划员 |

| | |
|---|---|
| 工作角色 ID | CO-OPL-003 |
| 专业领域 | 网络运营计划（OPL） |
| 类别 | 收集和操作（CO） |
| 工作角色描述 | 致力于推动网络运营合作伙伴之间跨组织或国家边界的合作。 通过提供指导，资源和协作来帮助合作伙伴网络团队的整合，以发展最佳实践并促进组织对实现综合网络行动目标的支持。 |
| 任务 | T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599 |
| 技能 | S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360 |
| 能力 | A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105 |

| | |
|---|---|
| 工作角色名称 | 网络运营商 |
| 工作角色 ID | CO-OPS-001 |
| 专业领域 | 网络运营（OPS） |
| 类别 | 收集和操作（CO） |
| 工作角色描述 | 进行系统的收集，处理和/或地理定位以利用，定位和/或跟踪感兴趣的目标。 执行网络搜索，战术取证分析，并在执行网络操作时执行。 |

| | |
|---|---|
| 任务 | T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609 |
| 技能 | S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363 |
| 能力 | A0095, A0097, A0099, A0100 |

## B.7 调查（IN）

| | |
|---|---|
| 工作角色名称 | 网络犯罪调查员 |
| 工作角色 ID | IN-INV-001 |
| 专业领域 | 网络调查（INV） |
| 类别 | 调查（IN） |
| 工作角色描述 | 使用受控和记录的分析和调查技术识别，收集，检查和保存证据。 |
| 任务 | [注：有些活动只能由执法或反情报局的人员进行。]<br>T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479，T0523 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, |

| | |
|---|---|
| | K0624 |
| 技能 | S0047, S0068, S0072, S0086 |
| 能力 | A0174, A0175 |

| | |
|---|---|
| 工作角色名称 | 执法/反间谍取证分析师 |
| 工作角色 ID | IN-FOR-001 |
| 专业领域 | 数字取证（FOR） |
| 类别 | 调查（IN） |
| 工作角色描述 | 对基于计算机的犯罪行为进行深入调查，建立文件或物理证据，包括与网络入侵事件相关的数字媒体和日志。 |
| 任务 | T0059, T0096, T0220, T0308, T0398, T0419, T0401, T0403, T0411, T0425 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0305, K0624 |
| 技能 | S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093 |
| 能力 | A0005, A0175 |

| | |
|---|---|
| 工作角色名称 | 网络防御取证分析师 |
| 工作角色 ID | IN-FOR-002 |
| 专业领域 | 数字取证（FOR） |
| 类别 | 调查（IN） |
| 工作角色描述 | 分析数字证据并调查计算机安全事件以获取有用的信息，以支持系统/网络漏洞缓解。 |
| 任务 | T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, |

| | |
|---|---|
| | T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546 |
| 知识 | K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347, K0624 |
| 技能 | S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156 |
| 能力 | A0005, A0043 |

# 附录 C – 劳动力开发工具

## C.1 DHS 网络安全劳动力开发工具包

美国国土安全部网络安全劳动力开发工具包（CWDT）[8]帮助任何组织了解其网络安全工作人员和员工需求，以保护其信息，客户和网络。该工具包包括网络安全职业路径模板和招聘资源，以招聘和留住顶尖的网络安全人才。 CWDT 提供的工具可帮助理解组织的网络安全人员风险并清点组织的员工队伍。CWDT 工具利用 NICE 框架中的专业领域，KSAs 和任务。CWDT 指出，准备建立网络安全人员队伍的第一步是组织网络安全人员的共同愿景。共同愿景支持领导者响应不断变化的环境，并提供数据以更好地调整资源，查看工作模式，突出潜在风险领域。这种理解在不断变化的网络安全环境中尤为重要。 CWDT 包括网络安全人力规划能力成熟度模型（CMM），这是一种自我评估工具，可帮助组织评估其网络安全人力规划能力的成熟度。

（CWDT）提供简介作为指导，重点关注各级别的工作人员，无论是入门级，中级职业还是经验丰富的网络安全专业人员。

### C.1.1 熟练程度和职业道路

与员工共同开发和分享职业道路将有助于他们确定自己的能力水平，并提升网络安全职业道路。

CWDT 包括为组织开发网络安全职业途径的三步过程。

- 第 1 步-熟悉熟练程度并审查样本职业道路。
- 第 2 步-使用 CWDT 模板为贵组织填写“建议的经验和证书”，“能力和样本技能/KSA”以及“建议的培训和开发活动”，为您的组织创建定制的网络安全特定职业路径。
- 第 3 步-与网络安全经理和员工分享职业道路。

## C.2 Baldrige Cybersecurity Excellence Builder 工具

一旦组织确定了其网络安全要求（例如通过网络安全审计或内部自我评估），它可以参考 NICE 框架来确定有助于满足这些要求的工作角色和任务。 尽管一般性术语（如“网络专业人士”）历来被用于衡量需求，但 NICE 框架提供的特殊性为描述所需的几十个离散工作职能提供了更好的方法。 通过确定所需的和可用的能力，并确定所需技能和可用技能之间的差距，组织可以确定关键需求。 NICE 框架可帮助组织回答以下来自 Baldrige Cybersecurity Excellence Builder 工具[9]的关于维护有效且支持人力环境以实现其网络安全目标的问题：

- 您如何评估与网络安全相关的员工能力和能力需求？
- 您如何组织和管理您的网络安全人员以建立角色和责任？
- 您如何准备员工以改变网络安全能力和容量需求？

随着越来越多的组织评估其网络安全人员队伍，NICE 框架中的通用词典支持多个组织，行业和地区的能力和能力评估。

## C.3 职位描述起草工具

DHS Cyberskills 管理支持倡议 PushbuttonPD 工具[10]允许管理人员，主管和人力资源专家迅速起草联邦员工职位描述（PD），而无需广泛的培训或对职位分类的预先知识。 它旨在呈现来自多个关键任务权威来源和职责，任务和 KSA 标准的语言，快速捕捉招聘官员的

要求，并将其呈现在可轻松整合到现有机构人力资源流程中的强大招聘包中。 任何组织都可以尝试使用 PushbuttonPD 工具来了解它如何将 NICE 框架材料纳入工作描述。

# 附录 D – 指南和指南文件的交叉参考

NICE 战略目标 3 指南职业发展和劳动力计划旨在支持雇主应对市场需求并加强网络安全人才的招聘，聘用，发展和留住人才。 这个战略目标的一个目标是发布和提高 NICE 框架的意识并鼓励采用。 在这种情况下的采用意味着 NICE 框架被用作与网络安全人员，培训和教育相关的行动的参考资源。

鼓励采用 NICE 框架的一种方法是推动网络安全指南或指南文档的作者将这些文档的一些内容交叉引用到 NICE 框架中的组件。 附录 D 包括可能鼓励采用 NICE 框架的出版物交叉引用的例子。

## D.1 网络安全框架

2014 年，NIST 发布了“改进关键基础设施网络安全框架”[11]，通常被称为网络安全框架。 为响应行政命令（EO）13636 [12]而开发的网络安全框架提供了一种基于性能和成本效益的方法，可帮助组织识别，评估和管理网络安全风险。 它是通过 NIST 召集的一系列公开研讨会而建立的，旨在更好地理解哪些标准和方法有助于实现有效的风险管理，以及如何实施自愿的现有良好实践以改善网络安全。

网络安全框架（NBS 改善关键基础设施网络安全路线图[13]）的配套文件指出，需要有熟练的网络安全人员来满足关键基础设施独特的网络安全需求。 它认识到，随着网络安全威胁和技术环境的演变，员工必须继续适应设计，开发，实施，维护和持续改进必要的网络安全实践。

网络安全框架由三部分组成：框架核心，框架实施层和框架配置文件。每个网络安全框架组件都加强了业务驱动因素和网络安全活动之间的联系。框架核心元素一起工作如下：

- 职能部门将最基层的网络安全活动组织起来。 这些功能 - 识别，保护，检测，响应和恢复 - 将在下面详细介绍。
- 类别是将功能细分成与计划需求和活动密切相关的网络安全成果小组。
- 子类别将类别进一步划分为技术和/或管理活动的具体结果。它们提供了一组结果，

虽然并非详尽无遗，但有助于支持各类别成果的实现。

- 信息性参考资料是关键基础设施行业常见的标准，准则和实践的具体部分，说明实现与每个子类别相关的结果的方法。 框架核心中提供的信息性参考是说明性的而不是详尽的。 它们代表了框架开发过程中经常提到的跨部门指导。

核心职能各自有助于高层次理解组织的网络安全需求：

- 识别（ID） - 开发组织理解管理系统，资产，数据和功能的网络安全风险。
- 保护（PR） - 制定并实施适当的保障措施，确保提供关键基础设施服务。
- 检测（DE） - 制定并实施适当的活动以确定网络安全事件的发生。
- 响应（RS） - 制定并执行适当的活动，以便就检测到的网络安全事件采取行动。
- 恢复（RC） - 制定并实施适当的活动，以维护恢复能力计划并恢复因网络安全事件而受损的任何功能或服务。

在很多方面，这些函数都与 NICE 框架类别相关。 表 8 描述了网络安全框架功能和 NICE 框架类别之间的关系。

**表 8 - NICE 框架劳动力类别与网络安全框架职能的交叉点**

| NICE 框架类别 | 类别描述 | 相关网络安全框架功能 |
|---|---|---|
| 安全准备（SP） | 概念化，设计和/或构建安全信息技术（IT）系统，并负责系统和/或网络开发的各个方面。 | 识别（ID），保护（PR） |
| 操作和维护（OM） | 提供确保有效和高效的信息技术（IT）系统性能和安全所需的支持，管理和维护。 | 保护（PR），检测（DE） |
| 监督和治理（OV） | 提供领导，管理，指导，发展和宣传，以便组织可以有效地开展网络安全工作。 | 识别（ID），保护（PR），检测（DE），恢复（RC） |
| 保护和防御（PR） | 识别，分析和减轻内部信息技术（IT）系统和/或网络的威胁。 | 保护（PR），检测（DE），响应（RS） |
| 分析（AN） | 对传入的网络安全信息进行高度专业化的审查和评估，以确定其对情报的有用性。 | 识别（ID），检测（DE），响应（RS） |

| | | |
|---|---|---|
| 收集和操作（CO） | 提供专业的拒绝和欺骗操作，并收集可用于开发情报的网络安全信息。 | 检测（DE），保护（PR），响应（RS） |
| 调查（IN） | 调查与信息技术（IT）系统，网络和数字证据相关的网络安全事件或犯罪。 | 检测（DE），响应（RS），恢复（RC） |

## D.1.2 网络安全框架与 NICE 框架的示例集成

虽然网络安全框架和 NICE 框架是分别开发的，但是每个框架都通过描述实现网络安全目标的分层方法来补充另一方面。 考虑下面的例子：

网络安全框架的响应功能包括缓解（RS.MI）类别。 该类别包括一个子类别 RS.MI-2，指出“事件得到缓解”的结果。虽然网络安全框架描述了这一结果，并提供了若干有关实现它的安全控制的信息参考，但网络安全框架没有提供任何关于谁应该负责实现结果的信息指导，或者 KSAs 将适用什么。

回顾 NICE 框架，我们确定了保护和防御（PR）类别事件响应（IR）专业领域中的网络安全防御事件响应者（PR-IR-001）角色。 我们可以回顾这个角色的描述，以确保它符合网络安全框架 RS.MI-2 的成果：

- 响应相关领域内的中断，以缓解直接和潜在的威胁。 使用缓解，准备和响应和恢复方法来最大限度地提高生存率，保护财产和信息安全。 调查和分析相关的应对活动，并评估现有做法的有效性和改进。
- 调查，分析并响应网络环境或飞地内的网络安全事件。

我们从本文件的附录 A 中了解到，其职位包括该工作角色的人可能会执行以下许多与期望的网络安全框架结果一致的任务：

- T0041-协调并为企业级网络安全防御技术人员提供专家技术支持，以解决网络安全防御事件。
- T0047-将事件数据关联起来以确定具体的漏洞并提出建议，以便迅速进行补救。
- T0161-对来自各种来源（例如，单个主机日志，网络流量日志，防火墙日志和入侵检测系统[IDS]日志）的日志文件进行分析，以确定可能的网络安全威胁。
- T0163-执行网络安全防御事件分类，包括确定范围，紧迫性和潜在影响;确定具体的漏洞;并提出可以迅速补救的建议。
- T0170-执行初步的，法医学上可靠的映射收集并检查以识别企业系统可能的缓

解/修复。

- T0175-执行实时网络安全防御事件处理（例如，法医收集，入侵关联和跟踪，威胁分析和直接系统修复）以支持可部署的事件响应小组（IRT）。
- T0214-接收并分析来自企业内各种来源的网络警报，并确定此类警报的可能原因。
- T0233-跟踪和记录从最初检测到最终解决方案的网络安全防御事件。
- T0246-撰写和发布网络安全防御技术，指导和事件发现报告给适当的选区。
- T0262-采用经批准的纵深防御原则和实践（例如，防御 - 多个地方，分层防御，安全稳健性）。
- T0278-收集入侵工具（例如，源代码，恶意软件，特洛伊木马）并使用发现的数据来缓解企业内潜在的网络安全防御事件。
- T0279-担任执法人员的技术专家和联络员，并根据需要解释事件详情。
- T0312-与情报分析师协调关联威胁评估数据。
- T0164-执行网络安全防御趋势分析和报告。
- T0395-撰写并发布行动后评论。
- T0503-监控外部数据源（例如，网络安全防御供应商站点，计算机应急响应小组，安全焦点）以维护网络安全防御威胁状况的货币并确定哪些安全问题可能对企业产生影响。
- T0510-协调事件响应功能。

此外，从附录 B 中，我们可以了解网络安全状况包括该工作角色的人可能需要的广泛的 KSA。

有了这些信息，一个试图实现网络安全框架所描述的结果的组织

RS.MI-2 可以确定一个或多个现有员工是否具备完成所述任务的必要技能。 如果缺少一个或多个 KSA，那么希望填补该工作角色的员工将具体了解哪些领域需要改进，并且可以寻求学术课程或行业培训以获得必要的知识。 如果没有找到这种工作人员，雇主就有具体的任务说明和 KSA 要求，这些要求可以在招聘公告中公布，也可以用于承包商工作人员来扩充现有人员。

## D.2 系统安全工程

美国国家标准与技术研究所特殊出版物（SP）800-160，系统安全工程-可信赖安全系统工程中多学科方法的考虑[14]，阐述了开发更多防御性和可生存系统所需的工程驱动行动-包括构成这些系统和依赖它们的服务。它从一套完善的系统和软件工程国际标准开始，并以此为基础，并将系统安全工程技术，方法和实践融入到这些系统和软件工程活动中。最终目标是根据利益相关方要求和保护需求的角度来处理安全问题，并使用已建立的工程流程来确保在系统的整个生命周期内以适当的尽责和严格度来满足这些要求和需求。提高系统的可信度是一项重要的任务，需要对系统，组件，应用程序和网络的需求，架构，设计和开发进行大量投资，并且对当前的“一切照旧”方式进行根本性的文化变革。

引入一套严格的，结构化的，基于标准的系统安全工程活动和任务提供了一个重要的起点和强制功能来启动所需的更改。 最终目标是获得完全有能力支持关键任务和业务运营的可靠安全系统，同时保护利益相关方资产，并且在保证水平与这些利益相关方的风险承受度一致的情况下实现。

将 NICE 框架的组件映射到 NIST SP 800-160 中描述的专业学科将验证这些组件。 系统安全工程专业学科的从业者可能会成为主题专家，他们可以证明额外的 KSA 和任务可以添加到 NICE 框架中。

## D.3 美国人事管理办公室联邦网络安全法规

2017 年 1 月 4 日，美国人事管理局（OPM）发布了一份备忘录[15]，标题为“联邦机构为具有信息技术，网络安全和网络相关职能的职位分配新的网络安全代码指南”。 该备忘录指出，2015 年联邦网络安全劳动力评估法[16]要求 OPM 制定程序以实施 NICE 编码结构，并确定所有需要履行信息技术，网络安全或其他与网络相关职能的联邦民事立场。 表 9 显示了代表网络安全工作跨学科性质的 NICE 框架工作角色 ID 到与 OPM 企业人力资源整合系统兼容的 OPM 网络安全代码的映射。

**表 9 - 工作角色 ID 与 OPM 网络安全代码的交叉点**

| 工作角色 ID | OPM 代码 | 工作角色 ID | OPM 代码 | 工作角色 ID | OPM 代码 |
|---|---|---|---|---|---|
| SP-PSK-001 | 611 | OV-LGA-001 | 731 | AN-TWA-001 | 141 |
| SP-PSK-002 | 612 | OV-LGA-002 | 732 | AN-EXP-001 | 121 |
| SP-DEV-001 | 621 | OV-TEA-001 | 711 | AN-ASA-001 | 111 |

| | | | | | |
|---|---|---|---|---|---|
| SP-DEV-002 | 622 | OV-TEA-002 | 712 | AN-ASA-002 | 112 |
| SP-ARC-001 | 651 | OV-MGT-001 | 722 | AN-TGT-001 | 131 |
| SP-ARC-002 | 652 | OV-MGT-002 | 723 | AN-TGT-002 | 132 |
| SP-TRD-001 | 661 | OV-SPP-001 | 751 | AN-LNG-002 | 151 |
| SP-SRP-001 | 641 | OV-SPP-002 | 752 | CO-COL-001 | 311 |
| SP-TST-001 | 671 | OV-EXL-001 | 901 | CO-COL-002 | 312 |
| SP-SYS-001 | 631 | OV-PMA-001 | 801 | CO-OPL-001 | 331 |
| SP-SYS-002 | 632 | OV-PMA-002 | 802 | CO-OPL-002 | 332 |
| OM-DTA-001 | 421 | OV-PMA-003 | 803 | CO-OPL-003 | 333 |
| OM-DTA-002 | 422 | OV-PMA-004 | 804 | CO-OPS-001 | 321 |
| OM-KMG-001 | 431 | OV-PMA-005 | 805 | IN-INV-001 | 221 |
| OM-STS-001 | 411 | PR-CDA-001 | 511 | IN-FOR-001 | 211 |
| OM-NET-001 | 441 | PR-INF-001 | 521 | IN-FOR-002 | 212 |
| OM-ADM-001 | 451 | PR-CIR-001 | 531 | | |
| OM-ANA-001 | 461 | PR-VAM-001 | 541 | | |

# 附录 E – 缩略语

本文中使用的缩写词和缩写定义如下：

API 应用程序接口

CDM 连续诊断和缓解

CDS 跨域解决方案

CIO 首席信息官

CKMS 加密密钥管理系统

CMMI 能力成熟度模型集成

CMS 内容管理系统

CNSSI 国家安全系统指令委员会

COMSEC 通信安全

COTR 签约官员的技术代表

DNS 域名系统

EISA 企业信息安全架构

FISMA 联邦信息安全现代化法案

FOIA 信息自由法

HR 人力资源

| | |
|---|---|
| DS | 入侵侦测系统 |
| IP | 互联网协议 |
| IPS | 入侵防御系统 |
| IR | 事件响应 |
| IRT | 事件响应小组 |
| ISD | 教学系统设计 |
| ITL | 信息技术实验室 |
| KSA | 知识，技能和能力 |
| LAN | 局域网 |
| NICE | 国家网络安全教育倡议 |
| OLA | 运营级别协议 |
| OMB | 管理和预算办公室 |
| OPM | 人事管理办公室 |
| OS | 操作系统 |
| OSI | 开放系统互连 |
| P.L. | 公共法 |
| PCI | 支付卡行业 |
| PHI | 个人健康信息 |
| PIA | 隐私影响评估 |
| PII | 个人身份信息 |
| PKI | 公钥基础设施 |
| R&d | 研究和设计 |
| RFID | 射频识别 |
| RMF | 风险管理框架 |
| SA&A | 安全评估和授权 |
| SDLC | 系统开发生命周期 |
| SLA | 服务等级协定 |
| SOP | 标准作业程序 |
| SQL | 结构化查询语言 |
| TCP | 传输控制协议 |

| | |
|---|---|
| TTP | 战术，技术和程序 |
| URL | 统一资源定位器 |
| VPN | 虚拟专用网络 |
| WAN | 广域网 |

# 附录 F – 参考文献


[1] NICE 框架修订网页，国家标准与技术研究所[网站]，https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurityworkforce-framework-revisions

[2] 国家网络安全教育倡议，国家网络安全劳动力框架，ver。 1.0，https://www.nist.gov/file/359276

[3]国家网络安全教育倡议，国家网络安全劳动力框架，ver。 2.0，https：//www.nist。gov / file / 359261

[4] NIST 特刊 800-181 的参考电子表格 https://www.nist.gov/file/372581

[5] NICE 框架，国家标准与技术研究院[网站]，https：// www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforceframework

[6]美国劳工部，就业和培训管理局（ETA）[网站]。 https://www.doleta.gov

[7] 能力模型信息交换机构，网络安全能力模型，https://www.careeronestop.org/competencymodel/competencymodels/cybersecurity.aspx

[8]美国国土安全部，网络安全劳动力开发工具包（CWDT），https://niccs.us-cert.gov/workforce-development/cybersecurityworkforce-development-toolkit

[9] 国家标准与技术研究院[网站] Baldrige 网络安全卓越计划，https://www.nist.gov/baldrige/products-services/baldrigecybersecurity-initiative

[10] 美国国土安全部，CMSI PushButtonPD™ 工具网站，https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[11]改进关键基础设施网络安全的框架 1.0 版，国家标准与技术研究院 2014 年 2 月 12 日，https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurityframework-021214.pdf

[12]行政命令第 13636，改进关键基础设施网络安全，DCPD-201300091，2013 年 2 月 12 日。http://www.gpo.gov/fdsys/pkg/FR-2013-0219/pdf/2013-03915.pdf

[13] NIST 改进关键基础设施网络安全路线图，国家标准与技术研究院，2014 年 2 月 12 日， https://www.nist.gov/sites/default/files/documents/cyberframework/ roadmap-021214.pdf

[14]美国国家标准与技术研究院，2016 年 11 月，NIST 特别出版物（SP）800-160，系统安全工程考虑， 用于可信赖安全系统工程的多学科方法， https://doi.org/10.6028/NIST.SP.800-160

[15]关于为信息技术，网络安全和网络相关职能职位分配新的网络安全守则的指导意见备忘录， 2017 年 1 月， https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codespositions-信息技术，网络安全

[16] H.R.2029 - 2016 年综合拨款法案，其中载有 2015 年司 N 网络安全法，https://www.congress.gov/114/plaws/publ113/PLAW114publ113.pdf