NIST 特别草案 800-181

NICE 网络空间安全人才框架（NCWF）

National Initiative for Cybersecurity Education (NICE)

国家网络空间安全教育计划

Bill Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

翻译：刘欢迎，姚振宇，黄惠

校对：莫雯希，刘江宁

湖南合天智汇信息技术有限公司

2017 年 4 月

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

NIST 特别草案 800-181

NICE 网络空间安全人才框架（NCWF）

National Initiative for Cybersecurity Education (NICE)

国家网络空间安全教育计划

Bill Newhouse
应用网络空间安全部
信息技术实验室（ITL）
Stephanie Keith
网络空间人才战略和政策司
国防部首席信息官办公室副主任
Benjamin Scribner
网络空间意识和教育局
国土安全部国家防护和计划司
Greg Witte
G2, Inc.公司
Annapolis Junction, MD

November 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

国家标准与技术研究所
Willie May，商务部副部长（主管标准和技术）

授权说明

本文档由 NIST 根据 2014《联邦信息安全现代化法案》（FISMA）、美国法典 44 U.S.C. § 3551 及公法 113-283 所规定的职责编写而成。NIST 负责制定信息安全标准和指导方针，包括对联邦信息系统的最低要求，但未经联邦有关部门明确批准和授权，这些标准和准则不能应用于国家安全系统。本指南符合美国行政管理和预算局（OMB）A-130 公告的要求。

本指南不得与商务部在法定授权下强制制定的、对联邦机构带有约束力的标准和指南相冲突。本指南不应被视为对商务部、OMB 办公室或其他联邦官方的现有授权的更改或替代。本指南可由非政府组织无偿使用，在美国不受版权保护。当然，如果注明出处，NIST 将不胜感激。

国家标准与技术研究所（NIST）SP 特别草案 800-181
NIST 草案标准 800-181 116 页（2016 年 11 月）
国际刊名代码：NSPUE2

为充分描述某个实验过程或概念，在本文中可能会提到某些商业实体、设备或材料名称，但并不意味着 NIST 推荐或认可它们，也不意味着这些实体、设备或材料是最适合的。
本文参考了 NIST 法定职责内正在编写的其他文档的内容。本文中的内容，包括概念和方法论，都可以在这些参考文档正式完成之前被联邦机构使用。因此，在每个文档完成之前，当前所规范的要求、准则和程序（如果存在）仍然有效。为了规划和转型需要，联邦机构可能希望密切跟进 NIST 这些新草案的制定情况。

鼓励所有企事业单位在公开征询意见期间，审查所有草案，并向 NIST 反馈。除了上述草案外，NIST 的其他网络空间安全草案可在 http://csrc.nist.gov/publications 获得。

公众意见征询期：2016 年 11 月 2 日至 2017 年 1 月 6 日
国家标准与技术研究所（NIST）
收件人：应用网络空间安全部（ACD）信息技术实验室（ITL）Bureau Drive 路 100 号（邮递点 2002）盖瑟斯堡，马里兰州（邮编：MD 20899-2002）
邮箱：ncwf@nist.gov

计算机系统技术报告

NIST 信息技术实验室（ITL）为国家测量和标准基础设施提供技术领导力，促进美国经济和公共福利的发展。ITL 致力于测试、测试方法、参考数据、概念验证实现和技术分析，推动信息技术的发展和有效利用。除了国家安全相关信息，ITL 负责制定联邦信息系统中其他所有管理、行政、技术和物理相关的标准和指导方针，以谋求高效益的安全和隐私保障。800 系列的特别草案汇总了 ITL 在信息系统安全上的研究、指南和开拓的成果，以及与工业界、政府和学术机构之间协作情况。

摘要

本文介绍了 NICE 网络空间安全人力资源框架（NCWF），该框架是人力资源培训和教育领域多年联合研究的产物。NCWF 提供了一个基础的参考资源，来描述和分享有关网络空间安全岗位角色、网络空间安全从业人员的岗位职责，以及所需的知识、技能和能力（KSAs）的信息。 NCWF 作为一个分类描述网络空间安全工作的通用的、统一的辞典，使得有关如何识别、招聘、培养和留住网络空间安全人才的沟通变得更加方便。NCWF 可以作为资源，帮助组织机构或私营部门制定更多出版物或工具，为网络空间安全人才的培养、规划、培训和教育提供指导。

关键词

能力；网络空间安全；网络空间；教育；知识；角色；技能；职责；培训；岗位角色

致谢

作者由衷感谢和赞赏一些公共或私有机构及个人为本文作出的重大贡献，他们周到的、富有建设性的意见提高了本文的整体质量、严密性和实用性。感谢国家标准与技术研究所(NIST)国家网络空间安全教育计划(NICE)负责人 Rodney Petersen 的领导和付出。特别感谢 Lynne Clarke, Ryan Farr, Jodi Guss, Lori Pfannenstein, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matt Smith, Bluma Sussman, Baris Yakin 和 Onika Williams 对本文的私人贡献。

2012 年 9 月，NCWF 第一次公开发表用于征集意见，2013 年 4 月，NCWF 第一版正式出版[1]。作者由衷肯定 Jane Homeyer 博士， Anne Quigley, Rex Min, Maya Yankelevich, 和 Peggy Maxson 主导了 NCWF 的发展完善，以及 Montana Williams 和 Roy Burgess 为 NCWF 版本 2.0 的研究开发引航领路[2]。

最后，作者充满敬意地感谢从上个世纪 60 年代开始，为计算机安全领域做出开创性贡献的人们。正是早期拓荒者的远见、洞察力和献身精神，奠定了本文所述的职责、知识、技能、能力的基础，解开有关网络空间安全人才的重要难题。

审阅提示

随着网络空间安全攻击的持续频发、强度和不良后果，对联邦、州政府、地方政府、军队、企业、工业和关键基础设施造成破坏，危害和威胁愈演愈烈，建立一支能够部署、提供、维护和发展网络空间安全的人才队伍，是保障美国经济和国家安全利益的当务之急。

- Bill Newhouse, NICE 副主任

商标信息

综述

国家网络空间安全教育计划（NICE）由美国商务部国家标准与技术研究所（NIST）牵头发起，该计划促进政府机构、学术界和私营部门形成合作伙伴，致力于加强提升网络健壮性并促成一个涵盖网络空间安全教育、培训和人才培养的健全生态系统。NICE 履行自己的使命，协调政府、学术界和工业伙伴基于现有成功项目形成合作，激励变革和创新，以培养壮大具备熟练技能的网络空间安全专业人才队伍为愿景，助力于保卫国家安全。

NICE 致力于培养全方位的网络空间安全人才，在整个职业生涯中始终具备全球竞争力，以保护我们国家免受已有或新兴网络空间安全威胁。尽管网络空间安全越来越受到关注和全球聚焦，许多管理者表示他们缺乏熟练的网络空间安全人才，并在雇佣合格人员填补网络空间安全缺口这一问题上亟需帮助。

因为网络空间安全的威胁以及防御系统一直在发展和演化，网络空间安全从业人员需要能够适应、设计、开发、实现、维护、度量和了解网络空间安全的所有领域。网络空间安全从业人员不仅包括那些专业的技术人员，而且包括那些运用网络空间安全知识去迎接固有挑战，确保他们效力的组织机构成功执行使命的人。一个具备充分理论知识、熟练掌握技能的网络空间安全人才能够实施和维护安全防护系统并采取相应措施，满足我们国家的安全需求。

本文作为一个基本参考，帮助组织机构组建一支满足网络空间安全需求的人才队伍。它介绍了 NCWF 如何为企业提供一个通用的、统一的词汇表来分类描述网络空间安全工作。本文定义了 NCWF 组件，即类别、专业领域和岗位角色。最后，介绍了每个网络空间安全岗位角色的职责集，以及位于该网络空间安全岗位的从业人员应展现的知识、技能和能力（Knowledge, Skills, and Abilities，简称 KSAs）。依托这些组件和 NCWF 提供的通用词汇表，网络空间安全工作的组织和交流将变得更加融洽。

NCWF 可以被当成一本网络空间安全从业人员词典，NCWF 消费者也可以将它作为其他人才培养、教育或训练的参考。例如，它提供了一个起点，并为制定学术道路、职业路径、职位描述和培训内容提供了标准。NCWF 有助于确保我们的国家能够教育、招聘、培训、发展并留住一批高水平的网络空间安全人才。它服务于网络空间安全生态链中的几种关键受众，包括：

- **雇主**——帮助他们评估网络空间安全工作人员，认清网络空间安全人员配置的关键缺口，并改进职位描述；
- **当前和未来的员工**——帮助他们探究职责和工作角色，帮助了解热门的网络空间安全工作和职位中，哪些网络空间安全岗位角色及相关知识、技能和能力当前正被雇主重视。招聘专员和就业顾问也可以将 NCWF 用作支援雇员和求职者的资源。
- **培训和认证提供商**——他们希望帮助当前和未来的网络空间安全从业人员获得和证明 KSA 能力；
- **教育提供者**——他们可以使用 NCWF 为参考，开发与 KSA 和职责相关的课程体系、教程、研讨会；
- **技术供应商**——他们可以认清与自己提供的服务和硬件/软件产品配套的网络空间安全岗位角色和特定的职能及 KSA。

作为一种调动信息技术（IT）、，网络空间安全和网络空间相关工作的机制，NCWF 通过以下组件帮助组织机构整理构造岗位角色和责任：

- **类别**——常见的网络空间安全职能的顶层分类；

- **专业领域**——网络空间安全工作的不同领域；
- **岗位角色**——IT、网络空间安全或网络空间相关工作最详细的分组，包括履行一系列任务必需具备的特定知识、技能和能力；
- **职责**——NCWF 的岗位角色执行某项业务时被委派的具体工作活动；
- **知识，技能和能力（KSA）**——履行职责所需要的素质，一般通过相关经验或基于绩效的教育和培训来体现。

NCWF 组件共同诠释网络空间安全领域的工作，从高阶层的工作到非常细碎的工作。每个类别包含多个专业领域，每个专业领域又包含一个或多个岗位角色。每一个岗位角色由众多的职责和 KSA 组成。提供巨细靡遗的组件有助于组织机构系统化地建立它们的网络空间安全人才体系，从而提高员工绩效，促进高效益的人力资源管理，形成持续的敏捷响应。

虽然 NCWF 的某些部分基于联邦政府项目，但是任何存在网络空间安全人才需求的组织机构都可以从中获得帮助，并可以按需定制 NCWF。

如上所述使用 NCWF，可以巩固组织机构网络空间安全人才队伍。对现有员工的投入，比如致力于培训和留住现有人才的举措，可以帮助组织机构应对并实现风险管控目标。由 NCWF 提供通用语言也有助于人才需求和外部框架的对接，如网络空间安全框架（CSF）[3]，美国劳工部能力模型[4]，美国教育部就业能力框架[5]和国家安全局（NSA）/国土安全部（DHS）网络防御国家卓越学术中心（CAE- CD）[6]知识单元。

NCWF 建立在数十年的行业研究基础上，研究关注如何有效将风险转化为有价值的系统化的电子和物理信息。网络空间安全战术是瞬息万变的，总是通过技术手段寻求新的方法来获得信息优势。因为人类在不断进步，我们实现网络空间安全的方法也将不断演变，NCWF 的组件也必须相应地不断更新。作为一个持续协作的方法，NICE 将定期参考收到的建议，并更新发布 NCWF 版本。此外，我们也会开发新的参考资料，与 NCWF 元素互相参照。在可能的范围内，数字化的参考资料也将发布至 NICE 的网站，作为运用 NCWF 的辅助资料和关联资料。

目录

表格目录

1 简介

国家网络空间安全教育计划（NICE）由美国商务部国家标准与技术研究所（NIST）牵头发起，该计划促进政府机构、学术界和私营部门形成合作伙伴，致力于加强提升网络健壮性并促成一个涵盖网络空间安全教育、培训和人才培养的健全生态系统。NICE 履行自己的使命，协调政府、学术界和工业伙伴基于现有成功项目形成合作，激励变革和创新，以培养壮大具备熟练技能的网络空间安全专业人才队伍为愿景，助力于保卫国家安全。

NICE 致力于培养全方位的网络空间空间安全人才，在整个职业生涯中始终具备全球竞争力，以保护我们国家免受已有或新兴网络空间安全威胁。

有很多国家层面的活动，聚焦于利用业务驱动指导网络空间安全行为，以及将网络空间安全风险视为组织机构风险管控的一部分。一个熟练的网络空间安全从业人员需要符合关键基础设施、企业以及业务技术系统和网络对网络空间安全技能的特殊要求。因为网络空间安全的威胁以及防御系统一直在发展和演化，网络空间安全从业人员需要能够适应、设计、开发、实现、维护、度量和了解网络空间安全的所有领域。网络空间安全从业人员不仅包括那些专业的技术人员，而且包括那些运用网络空间安全知识、迎接固有挑战，确保他们效力的组织机构成功执行使命的人。一个具备充分理论知识、熟练掌握技能的网络空间安全人才能够实施和维护安全防护系统并采取相应措施，满足我们国家的安全需求。

今天的系统和网络是一个各种技术（比如硬件、软件和固件）、流程和人员的复杂集合体，它们协同工作来让组织机构有能力以更及时、更安全的方式来处理、存储和转换信息，以支撑各种各样的任务和业务功能。组织机构对利用这些系统和网络来达成日常的、重要的和关键的任务和业务功能的依赖程度，意味着保护这些基础系统和业务环境对组织机构的成功来说，是至关重要的。

为信息系统选择合适的安全和隐私控制策略始终是一个重要课题，它可能对组织机构的业务和资产以及个人福利产生重大影响。发现那些有能力选择、维护、评估、实施和升级合适的安全和隐私控制策略，并且具备知识、技能和能力的合格人员是一个挑战。这一点已经被越来越多的组织机构认识到。他们现在明白网络空间安全的风险只有靠那些有能力、有准备的网络空间安全人才才能解决。

了解如何培养和留住人才，让组织机构可以专注于它们自己业务和资产的网络安全风险，同时专注于个人的、其他机构的、甚至是国家的网络安全风险，这是非常重要的。合格的网络空间安全人才在全球互连的数字信息和通信基础设施中也是至关重要的，这些基础设施几乎支撑了现代社会的方方面面、并且为美国经济、民用设施、公共安全和国家安全提供重要支持。

1.1 NCWF 背景

NCWF 的概念在 NICE 建立之前就有了，这个概念在过去网络空间安全从业人员（联邦和私营组织机构）无法被衡量、我们国家网络空间安全所需岗位尚无定义的背景下就应运而生。为填补这一空白，联邦 CIO 委员会在 2008 年受命提供一个标准框架，来了解联邦政府内的网络空间安全角色。

2008 年，联邦 CIO 委员会发布了一个研究报告。这个报告参考了一些正在发展的信息技术专业发展的成果和政府机构需要的特定网络空间安全岗位角色的信息。

2011 年，13 种岗位被联邦 CIO 委员会识别并发布出来，这些内容由许多联邦机构相

关专家组成的专家组研究得出。

在这项工作的基础上，2011 年 9 月 NCWF 的第一个版本发布出来，并进行公开意见征集。

2013 年这些征集的意见被采纳形成一个新的版本，它成为了美国人事管理办公室（OPM）网络空间安全功能规范的基本依据。使用这些规范可以帮助联邦机构鉴别网络空间安全人才，判定能力基准，调查用人趋势，认清技能空缺，从而更高效地招聘、雇佣、培养和留住有价值的网络空间安全人才。

NCWF 的第一个版本进行了政府范围的审查，允许其他机构提出建议，并依据建议进行版本修订。美国国土安全部（DHS）分析了这些建议，并通过焦点讨论小组进行了最终建议验证。这些焦点讨论小组由来自全国各地的，包括私营组织机构、学术界和政府机构在内的相关专家组成。

DHS 焦点讨论小组的一个重要关注点就是去收集各个行业的建议，从而确保 NCWF 在全国范围内都是适用的，而不仅限于政府机构。作为结果，NCWF 第二版经过起草、验证，于 2014 年正式发布。

2014 年以来，美国国防部（DoD）进一步完善 NCWF，并新增了岗位角色（Work Role）这个概念——这在 NCWF 中是第一次出现。通过它体现更多的专业特征，帮助组织机构使用 NCWF 更好地定位网络空间安全的职位。DoD 从私人组织机构和政府收集了大量的有关岗位角色的提案建议，DHS 完善了这些提案，确保它们对于私人部门民用政府机构同样适用。

1.2 目的和适用范围

本文档目的是为组织机构等用人机构提供一个网络空间安全从业人员必备能力的基本参考。主要包括

- 为组织机构提供一个通用的、统一的词汇表，用它来分类和描述网络空间安全工作。
- 将网络空间安全工作划分为 7 个大类别。这 7 个类别中包含了超过 50 种岗位角色。
- 对每个岗位角色提供了一个相关工作的集合。
- 对每个岗位角色提供了一个相关知识、技能和能力（KSA）的集合。

使用 NCWF 作为参考，可以在鉴别、招聘、培养网络空间安全相关从业人员时提高沟通效率。NCWF 将让雇主使用更加精准、统一的语言，比如在专业开发项目中，在他们使用行业认证时，以及在为他们的从业人员选择相关的培训时。

NCWF 促使组织机构使用一种更具一致性、可比性、复用性的方法去挑选和规范网络空间安全职位角色。 它也提供了一个通用的词汇表，高等院校可以基于此来开发网络空间安全相关课程。这将有助于培养学生们满足当前和未来的网络空间安全人才需求。NCWF 作为一种资源被人们利用，意味着它有能力对所有网络空间安全相关工作提供解释说明。

NCWF 作为一种人们使用的资源，意味着它有能力对所有网络空间安全相关工作提供解释说明。NCWF 的适用性目标是任何一项网络空间安全工作或职位，都可以被 NCWF 定义的相关组件来识别和描述。有工作或职位支撑的任务或业务流程场景，将带动 NCWF 被选中的那些组件的发展。本文并不试图给出*网络空间安全*的定义，因为这个术语的使用经常依赖于组织机构的使命和业务上下文环境而不断变化。

组织机构可以将 NCWF 作为资源，制作出更多的出版物或工具，为人才的培训、规划、训练和教育的各个方面提供定义或指南。

1.3 读者/NCWF 消费者

NCWF 可以被当成一本网络空间安全从业人员词典，NCWF 消费者也可以将它作为参考，用于其他人才培养、教育或训练。NCWF 是一个有助于确保我国能够教育、招聘、训练、培训和留住高素质的网络空间安全人员的重要资源。

1.3.1 雇主

使用 NCWF 通用的词汇表，可以帮助雇主建立标准，梳理和培养他们的网络空间安全从业人员。

NCWF 可以被雇主和组织机构的领导层用来：

- 编目、跟踪他们的网络空间安全从业人员，更好地掌握他们在知识、技能、能力以及工作表现上的优势和欠缺。
- 确定培训和任职要求，为执行网络空间安全任务目的，提升关键的知识、技能和能力。
- 使用 NCWF 指定的岗位角色、选择相应的 KSA 和职责，优化职位描述和招聘启事。
- 制定最贴切的岗位角色和职业发展规划，引导员工掌握这些岗位角色所需的技能。

图 1 描述了 NCWF 如何助力建设强大的网络空间安全人才队伍。

图 1 -有能力、做好准备的网络空间安全人才模块图

如图所示，几项关键投入提高了 NCWF 的收益和价值，打造有能力、做好准备的网络空间安全人才。

- 通用的词汇表可以让教育工作者、雇主和雇员使用统一的专业术语。
- 关键性分析有助于识别那些构成基准的职责和 KSA（比如它们对多个岗位角色非常重要或者对于特定的基于角色的培训非常重要。）也有助于识别那些对岗位角色取得优秀绩效至关重要的职责和 KSA。
- 熟练度分析有助于合理地预期人员在一个岗位角色下展现的所述 KSA 的水平，比如，一个人在同一给定岗位角色下可能展现不同的理解力和能力，因为员工从入门到成为专家是循序渐进的过程。熟练度考量是从业人员考核的一个重点，NCWF 未来将考虑把它纳入到附加概念中，这一点将在 4.1 节阐述。

1.3.2 当前和未来的网络空间安全工作者

NCWF 支持那些已经进入或希望进入网络空间安全领域的人，探索网络空间安全领域各种类别和各种岗位角色的工作。它也同样可以帮助那些在工作者背后作为支持的人，比如招聘专员和就业顾问，他们帮助求职者和学生了解在热门的网络空间安全工作和职位中，哪些网络空间安全岗位角色及相关知识、技能和能力当前正被雇主重视。

当职位空缺公告和职位公开说明使用 NCWF 的通用词汇进行描述，对网络空间安全工作职责和职位所需的培训提供清晰、统一的说明，这些工作者将更加受益。

当培训机构和行业认证机构使用 NCWF 的通用词汇，那些已经进入或想要进入网络空间安全领域的人，就能找到那些可以帮助他们学习必备工作技能的培训机构和/或行业认证机构，从而获得一份网络空间安全的工作或晋升到一个新职位。使用通用词汇有助于学生和专业人员获得特定网络空间安全岗位角色的在职人员通常示范的 KSA 信息。了解这些信息可以帮助他们找到学术课程。这些课程的学习成果和知识单元所匹配的 KSA 和职责正是雇主所重视的。

1.3.3 教育工作者/培训讲师

NCWF 为教育工作者提供了一个参考，可以用来编写课程大纲、训练计划、教材、组织研讨会，以及练习和挑战那些在 NCWF 中描述的 KSA 和职责。

招聘专员和就业顾问可以将 NCWF 作为就业研究的资源。

1.3.4 技术提供商

NCWF 允许技术提供商鉴定与他们的软硬件产品、服务相关的网络空间安全岗位角色、职责和 KSA。

1.4 本文组织大纲

本文剩余章节的结构如下：

- 第二章定义 NCWF 的组件：（1）类别（2）专业领域（3）岗位角色（4）关联任务集（5）每个岗位角色的知识、技能和能力。
- 第三章通过与可适用的外部模型的交叉对照图展示 NCWF 的适用性。
- 第四章介绍 NCWF 将定期进行修订的流程。
- 附录 A 描述 NCWF 的类别、专业领域、岗位角色、职责和 KSA 列表。
- 附录 B 提供每一个岗位角色的详细列表，包括了对应的职责和 KSA。
- 增加的附录说明了使用的缩写和参考资料。

2 NCWF 组件和关系

2.1 NCWF 组件

NCWF 规整了信息技术（IT）、网络空间安全和网络空间领域的相关工作。本章介绍和定义支撑上述领域运作的 NCWF 核心组件。

2.1.1 类别

类别（Category）提供了 NCWF 的顶层组织结构。NCWF 一共有 7 个类别，每个类别都由专业领域（Specialty Area）和岗位角色（Work Role）组成。这种组织结构是在大量的工作职位分析的基础上得出，这些分析忽略了职位头衔和其他职业术语，而是依据主要工作职能的共性进行组别区分。

2.1.2 专业领域

各个类别下包含的网络空间安全工作分组——被称为专业领域（Specialty Areas）。在 NCWF v1.0 中有 31 个专业领域[1]，在 v2.0 中有 32 个专业领域[2]。每个专业领域代表了网络空间安全领域的一类专门工作职能。NCWF 的以往版本给每个专业领域定义了典型的工作职责和知识、技能和能力（后三者简称 KSA）。同一个给定类别下的各个专业领域之间，比起跨分类的另外专业领域，存在更多的相似性。在本文中，工作职责和 KSA 现在都与附录 A 中定义的岗位角色挂钩。

2.1.3 岗位角色

岗位角色（Work Role）是 IT、网络空间安全或网络空间相关工作最细化的分组。岗位角色阐明了从业人员完成规定职能和职责所必须具备的知识、技能和能力。

作为网络空间安全从业人员，在执行任务或业务时，只需从 NCWF 选择和职位相关的一个或多个岗位角色，依照职责描述履行工作。

为了便于组织管理和沟通网络空间安全工作的责任，岗位角色隶属于特定的类别和专业领域，如下文所述。

2.1.4 任务

每个岗位角色都需要个人来履行一定的职责或任务。职责相当于一类工作，它可以被分配给 NCWF 某个岗位角色下的专业人员。

2.1.5 知识、技能和能力

知识、技能和能力（KSA）是完成一项工作必需的属性，一般通过相关的工作经验、教育背景或培训经历体现。NCWF 将岗位角色与 KSA 挂钩，为每个岗位角色清晰定义了胜任该职责和职能所必需具备的任职资历和能力。

2.2 NCWF 组件关系

用多个 NCWF 组件来描述信息技术（IT）、网络空间安全和网络空间相关工作。如图 2 所示，每个类别下有多个专业领域的分支，每个专业领域下又有多个岗位角色的分支，每个岗位角色又是由大量独立的工作职责和与之对应的 KSA 组成。特别说明的是，KSA 序号 K0001 到 K0006 是所有网络空间安全活动的核心，适用于每一个岗位角色。

使用这种方式对组件分组，有助于组织管理岗位角色和对应的任务与 KSA，简化网络空间安全话题的交流，方便与外部框架对接。各个岗位角色对应的具体职责、知识、技能和能力见附录 B。

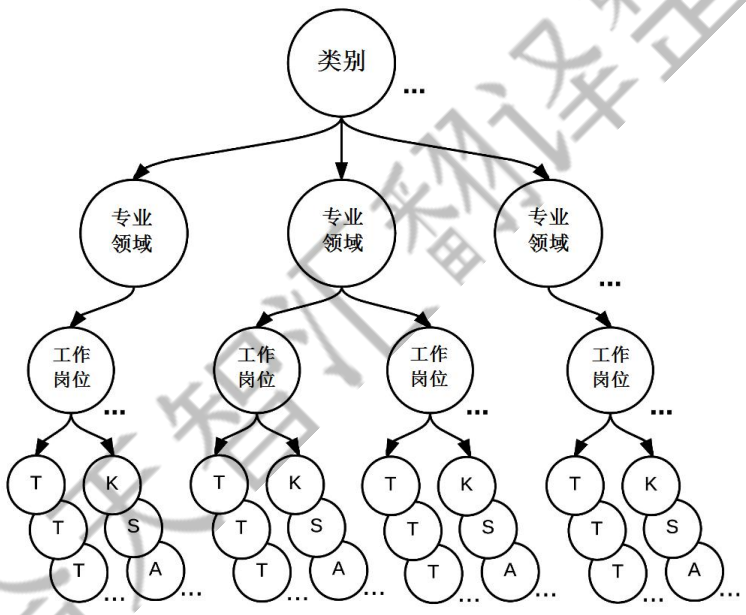

图 2 NCWF 组件关系图

3 NCWF 的应用

在第二章描述的各种组件的应用，让组织机构受益匪浅。使用 NCWF 了解组织机构的需求并评估这些需求的满足程度，帮助组织机构去规划、实施和监控一个卓越的网络空间安全计划。下面的论题阐述了如何利用 NCWF 达到这些业务目标，确保有效的绩效、高性价比的人力管理和持续保持网络空间安全能力处于就绪状态。虽然这几个例子都是专为联邦政府项目而制定的策略，但是任何对网络空间安全人才有需求的组织机构都可以从这些规则中获益。以下论题对于所有涉足网络空间安全人才发展事业的人们而言，都是非常有用的。

3.1 认清网络空间安全人才需求

随着科技成为当前社会几乎任一环节都不可或缺的关键要素，网络空间安全技术领域正在快速更新、蓬勃发展。技术的发展要求一批熟练的技术人员作为中坚力量帮助组织机构履行网络空间安全的职能。当组织机构认清了充分的风险管控在什么时机需要哪些东西后，领导者就需要考虑所需人才的数量和能力。

美国国土安全部网络空间安全人才培养工具包（CWDT）[9]——提供了帮助组织机构了解并建设他们的网络空间安全人才队伍的工具和指南。CWDT 阐述了建设网络空间安全人才队伍的准备工作的第一步，就是拥有一个共同的愿景，以此来统筹你的网络空间安全人才承担网络空间安全工作。拥有一个共同的认知可以帮助领导者应势而谋——给你数据以更好地调整资源，观察工作模式，关注潜在风险。这种认知在日新月异的网络空间安全环境中显得尤为重要。CWDT 提供了一个网络空间安全人力规划能力成熟度模型（CMM），这是一个可以自我评估的工具，可以帮助组织机构评估他们网络空间安全人才规划能力的成熟度。

一旦组织机构明确了网络空间安全需求（比如通过网络空间安全审计或者内部自我评估），NCWF 可以帮助他们找到实现这些需求的相关岗位角色和职责。虽然长期以来，我们用普遍的术语（例如“网络空间专家”）来估量需求，但是 NCWF 的独特之处在于，它提供了一个更好的方法来描述许多个相互独立的工作的必要职能。通过定义所需的和已有的资源的能力素质、通过认清所需的和已有的技能之间的差距，组织机构可以明确关键需求。NCWF 帮助组织机构回答以下问题，这些问题摘自波多里奇网络空间安全卓越构建工具（Baldrige Cybersecurity Excellence Builder Tool ）[10]，该工具是关于如何维护一个高效的、受拥护的人才环境，从而达到网络空间安全目标。

- 如何评估你的雇员能力和在网络空间安全方面的人力需求。
- 如何组织和管理你的网络空间安全人员，针对他们建立岗位角色和职责要求。
- 如何准备好你的网络空间安全人才的能力及数量以应对不断变化的网络空间安全环境。

网络空间安全的领域一直在不停演化，鉴于此，NCWF 对这些需求提供持续的监测，将其作为前瞻性风险管控办法的一部分。

3.2 教育和培训网络空间安全人才

接受信息安全教育和培训的人数近年来有显著增长，这在一定程度上归功于联邦政府在改善和扩大正规网络空间安全教育项目上所做的努力。尽管取得了这些成绩，但是许多机构逐渐发现，这些项目并不足以让学生充分满足岗位角色的需求。NCWF 通过统一的词汇，帮助教育工作者传授给学生那些岗位角色所规定的网络空间安全职位必备的专门知识、技能和能力。

高等院校是培养教育网络空间安全人才的重要部门。类似 NICE 计划，通过公有机构和私有机构之间的合作，让这些机构确定他们需要的常用知识和能力。反过来，NCWF 辞典的配套课程的开发和交付，让这些机构能更好地培养学生，使其足以胜任网络空间安全相关职位。随着学生们陆续发现心仪的网络空间安全岗位角色在增加，更多的学生将会被学校的网络空间安全计划吸引，并把它作为职业生涯的可靠途径。这方面的一个成功例子就是 NSA/DHS 的网络防御国家卓越学术中心（CAE-CD）计划办公室，它开发了一个演示[6] CAE-CE 知识点与 NCWF 关系的映射文档。

3.3 招聘和雇佣高水平的网络空间安全人才

由于网络空间安全的相关评估（比如信息安全审计）让组织机构知晓风险管控的优先级，对应 3.1 节描述的人力评估，NCWF 的应用将会帮助组织机构更好地实现战略性的人才规划和招聘。NCWF 的定义可以用来创建或修订职位描述，只需参照岗位角色依葫芦画瓢，NCWF 辞典则帮助求职者准确地找到他们感兴趣且能胜任的特定职位。通过使用 NCWF 的职责定义来描述工作职位的责任和职责，使用 NCWF 的 KSA 来描述职位需要的技能和资格要求。无论是求职者还是招聘经理都可以获得一个统一的期望值。这些标准的应用也有助于完善审查和核准求职者的评估标准。

美国国土安全部的 CMSI PushbuttonPD™ 工具[11]，让管理者、监事和人力资源专员可以迅速地拟定一份联邦员工职位描述（Position Description，简称 PD），而不需要大量的培训和预先掌握职位分类知识。它的宗旨是呈现多元的关键权威来源的语言，提出职责、任务和 KSA 的标准，快速地捕获招聘方的需求，这些需求被浓缩为一个强大的招聘方案包，可以轻易地与现有人力资源业务流程进行整合。

NCWF 的应用并不只限于外部招聘。因为它提供因人而异的培训建议和绩效评测，NCWF 框架可以帮助组织机构对现有员工进行再培训，使他们能够胜任网络空间安全的岗位角色。NCWF 也可以帮助组织机构获得临时的或长期的外聘员员工的补充，以填补 3.1 节所述的职位空缺。也可以让组织机构获得外力支持，帮助他们进行教育和培训，确保内部候选人最终具备必要的知识和技能。

3.4 留住和培养高水平的网络空间安全人才

一个成熟的网络空间安全人才计划的重要环节，包括留住并培养在职的高水平人才。一个在职员工已经拥有的人际关系、组织机构文化和组织经验是难以替代的。在一个员工离职后再招聘新人接手这个岗位，通常导致新的广告和招聘成本、培训的花费、生产率的降低以及员工士气的下降。美国国土安全部的 CWDT[9]工具提供了指南资料，关注于如何留住员工，无论他处于入门级水平、职业发展期还是经验丰富的专业人员。以下列表阐明了 NCWF 留住和发展网络空间安全人才的若干方法：

- 既然一些员工认识到网络空间安全是一个令人兴奋的技术领域，广泛的岗位角色和专业领域带来了大量的网络空间安全功能要求，这些都是他们梦寐以求并期望通过实践获得的。
- 虽然一些组织机构已经能够吸引网络空间安全人才，但能否留住这些人才将在一定程度上取决于能否提供更富挑战性并不断发展的一系列岗位角色，如同 NCWF 所列举的。
- 详细了解 NCWF 规范的职责和 KSA，有助于员工按照特定步骤为心仪的岗位做出相应努力，提升他们的能力，加强知识储备。组织机构甚至可能将员工转岗至这些岗位，让他们在 KSA 的实践中提高自己。
- 了解 NCWF 规范的职责和 KSA，有助于组织机构组织集体培训，使众多员工为履行特定类别、特定专业领域和特定岗位角色做好准备。
- KSA 有助于组织机构了解哪些技术能力能对位于特定网络空间安全岗位角色的员工有益。在获取了知识认证的基础上，组织机构可以开展基于网络空间安全技能和能力的培训和考试，比如在实操环境下考察 KSA 的熟练程度。
- 考虑到 3.1 章节识别出的员工在网络空间安全能力上的差距，组织机构可以使用现

有人员来填充关键的网络空间安全人员需求，重新审查现有人员的简历，从中找到那些具备现在急需 KSA 的人。

- 组织机构可以观察那些勤于提升相关 KSA 的员工，奖励那些有效完成任务的员工，并为那些需要特殊工作技能的员工制定改善计划。
- NCWF 可以帮助那些想要转岗至网络空间安全相关岗位角色的在职员工（比如一个在濒临淘汰的非网络空间安全岗位角色上的可靠员工，或者一个想要接受更多工作挑战的员工）。通过找准一条富有挑战性的职业道路，员工的热情可能被新的工作机会鼓舞，同时充分认识到 KSA 将帮助他们迎接新的角色。

如上所述使用 NCWF，可以巩固组织机构网络空间安全人才队伍。对现有员工的投入，比如致力于培训和留住现有人才的举措，可以帮助组织机构应对并实现风险管控目标。

3.5 网络空间安全框架(CSF)

2014 年 NIST 发布了关键基础设施网络空间安全提高框架[3]，通常被称为网络空间安全框架（CSF）。为了响应 13636 号总统行政令[12]，CSF 发展出一套提供基于绩效的、成本效益比好的方法，帮助组织机构来识别、评估和管理网络空间安全风险。该方法由 NIST 召开的一系列公开研讨会研究确立，研讨会的目的是为了更好地了解哪些标准和方法论能实现高效的风险管控，现有的自发的优秀实践将如何提升网络空间安全。

CSF 主要包括 3 个部分：核心框架、框架实现层和框架配置文件（每个配置文件都是一个组织机构根据自身需求选择的类和子类的集合）。每个部分都加强了业务驱动和网络空间安全活动之间的联系。CSF 与 NCWF 最密切相关的是它的核心框架部分。CSF 核心框架元素按以下方式工作：

- 功能（Function），主要把基础的网络空间安全活动按照它们最高层次的方式组织起来。这些功能包括——识别、保护、检测、响应和恢复，这些功能将在后面详细描述。
- 类别（Category）是功能的细分，主要是一些紧密联系可满足功能需求和特定活动的网络空间安全产出项的分组集合。
- 子类（Subcategory）是将类别根据具体的技术和/或管理行为的产出结果进一步细分。他们提供了一个结果集（虽然并不全面）来帮助达到每个类别中要求的产出结果。
- 参考文献（Informative Reference）是常见关键基础设施部分的标准、指南和实践的特定章节，描述了实现每个子类对应产出结果的方法。这个核心架构的参考文献是说明性的，并不详尽。它们主要着眼于依据框架开发过程中最常见的问题来设计跨行业指南。

一个指南文档——*NIST 改善关键基础设施网络空间安全路线图（NIST Roadmap for Improving Critical Infrastructure Cybersecurity）*[13]，论述了包括产业合作在内的 CSF 的发展史和联盟阵营的重要节点。这个计划基于利益相关者在整个开发过程中给出的反馈，包括了那些妨碍网络空间安全从业人员组织和沟通的因素。路线图指出了对一个熟练的网络空间安全从业人员的要求，以满足关键基础设施独有的网络空间安全需求。路线图指出，随着网络空间安全威胁和技术环境的不断演变，网络空间安全从业人员也必须不断地更新设计、开发、实现、维护技能，并且持续加强必要的网络空间安全实践。

每一个核心功能（Function）都有助于从更高层面了解组织机构的网络空间安全需求。

- **识别（ID）**—培养对管理系统、资产、数据和性能的网络空间安全风险的系统化的认识。

- **保护（PR）**—开发并实施适当的保障措施，确保关键基础设施服务的交付。
- **检测（DE）**—开发并实施适当的举措，检测网络空间安全事件的发生。
- **响应（RS）**—开发并实施适当的举措，应对检测发现的网络空间安全事件。
- **恢复（RC）**—开发并实施适当的举措，保持系统的恢复能力，在面对网络空间安全事件时确保系统能修复受损性能和服务。

在许多方面，CSF 的功能（Function）与 NCWF 的类别（Category）相对应，表格 1 描述了两者之间的关系。

表格 1 NCWF 人才类别与 CSF 功能对照表

NCWF 类别	类别描述	CSF 相关功能
安全基础设施提供	概念化、设计、建造安全的 IT 系统，负责系统和/或网络各个方面的开发	Identify (ID), Protect (PR)
运营与维护	为 IT 系统高效安全运行提供支持、管理和保障能力。	Protect (PR), Detect (DE)
监管与治理	提供领导、管理、指导或发展和倡议，让组织机构更有效的进行网络空间安全工作	Identify (ID), Protect (PR), Detect (DE), Recover (RC)
保护与防御	识别、分析、降低内部 IT 系统和/或网络的威胁	Protect (PR), Detect (DE), Respond (RS)
分析	对进来的网络空间安全信息进行高度专业化的审查和评估，以决定情报的价值。	Identify (ID), Detect (DE), Respond (RS)
搜集与运作	提供专业化的侦查和欺骗手段，收集可以作为情报的网络空间安全信息。	Detect (DE), Protect (PR), Respond (RS)
调查	针对 IT 系统、网络以及数字证据相关的网络空间安全事件和犯罪进行调查。	Detect (DE), Respond (RS), Recover (RC)

3.5.1 CSF 与 NCWF 的集成示例

虽然 CSF 和 NCWF 都是独立开发的，但是通过分层次描述的方法，两者互相补充，以实现网络空间安全的目标。请看下面的例子：

CSF 的**检测**（Detect）功能包括一个**安全持续监控**（**DE.CM**）的类别。这个类别包含一个子类 **DE.CM-1**，指向了一个产出结果“对网络进行监控来检测潜在的网络空间安全事件”。CSF 描述了这个产出结果，并且提供了关于安全控制的几个详细参考资料用来实现该产出结果，但是 CSF 并没有提供谁应该负责实现这个产出结果，以及需要运用哪些 KSA。

核查 NCWF，我们在**保护和防御（PR）**类别、**事件响应（IR）**专业领域下面的发现“**网络空间安全防御事件响应（PR-IR-001）**”角色。现在我们可以审视这个角色的描述，确保它与 CSF **DE.CM-1** 产出结果是匹配的。

对相关领域的破坏进行响应，减轻当前和潜在的威胁。使用减灾、防灾和响应与恢复的方法最大化挽救系统寿命、保护财产和信息安全。对相关的响应行为进行调查分析，评估现

有实践的有效性和完善性。

在网络环境或飞地内，对网络空间安全事件进行调查、分析和响应。

我们从本文的**附录 A** 了解到，处于该岗位角色的人将被预期履行以下多项职责。这些职责与 CSF 预期产出结果挂钩：

- T0041 –协调企业范围内的网络空间安全防御人员，并提供专业技术支持，帮助他们处理网络空间安全防御事件。
- T0047 – 关联网络空间安全事件数据用于识别特定漏洞，并针对快速修复给出建议。
- T0161 - 从多个来源进行日志分析（比如单个的主机日志，网络流量日志，防火墙日志，入侵侦测系统（IDS）日志），识别网络空间安全可能存在的威胁。
- T0163 -对网络空间安全防御事件进行分诊，包括确定范围、紧急程度和潜在影响，识别特定漏洞，并针对快速修复给出建议。
- T0170 – 在企业系统的进行初始的可靠的图像证据搜集，检查得出可行的缓解/修复措施。
- T0175 - 进行实时网络空间安全防御事件处理（例如数字取证，入侵关联和跟踪，威胁分析和直接系统修复）任务，来支持事件响应小组（IRT）
- T0214 - 接收、分析企业内各种来源的网络告警，并且确定引发这些告警的可能原因。
- T0233 -从网络空间安全防御事件的最初检测到最终解决，都进行跟踪并做好文档记录。
- T0246 –基于网络空间安全事件的调查结果，编写并发布网络空间安全防御技巧、指南和报告给适当的人员。
- T0262 –采用经过批准的纵深防御原则并实践（比如多地防御、分层防御、安全健壮性）
- T0278 - 在企业内，收集入侵文件（比如源代码、恶意软件、木马），利用已发现的数据降低潜在的网络空间安全防御事件的风险。
- T0279 - 作为技术专家与执法人员沟通，按照规定说明事件细节。
- T0312 –配合情报分析师对威胁评估数据进行关联分析
- T0333 - 进行网络空间安全防御趋势分析和汇报。
- T0395 - 编写和发布事后总结报告
- T0503 - 监控外部数据源（例如网络空间安全防御厂商网站，计算机应急响应团队，安全焦点），保持网络空间安全威胁防御环境的流通，并确定哪些安全问题可能对企业产生危害。
- T0510 - 协调事件响应职能。

此外，从**附录 B** 中我们可以看到更多网络空间安全从业人员所处岗位角色的 KSA 信息。

有了这些信息，组织机构在谋求实现 CSF **DE.CM-1** 描述的产出结果时，就可以确定是否有一个或多个员工具备完成这些职责所需的技能。当欠缺一个或多个 KSA 时，那些希望填补这个岗位角色的员工可以明确知道，需要提高哪些方面的能力，他可以寻找学术课程或行业培训来获取所需的知识。如果没有这样的员工，雇主可以把这些任务描述和 KSA 需求明确地写在招聘广告中，或者用于引进合同工以扩大现有劳动力。

4 未来改版流程

NCWF 建立在数十年的行业研究基础上，研究关注如何有效地将风险转化为有价值的系统化的电子和物理信息。这些年来，这个曾经被称为*计算机安全*、*信息安全*到现在被称为*网络空间安全*的行业，已经被众多充满奉献精神的从业者，以及不断演化的岗位角色、职责和 KSA 支撑起来。网络空间安全战术是千变万化的，总是通过技术手段寻求新的方法来获得信息优势。正因为我们不断演变实现网络空间安全的方法，NCWF 的组件也必须相应地不断更新。

我们鼓励 NCWF 用户通过 NICE 项目网站[14]的人才框架主页提供反馈意见和评论。作为一个持续协作的方法，NICE 将定期参考当前建议，对部分内容进行扩展、更新/修订、撤回、或整合。这项计划将努力在这些建议上达成共识，借助于包括联邦网安人才和教育领导者在内的公共部门和私有单位的力量，NCWF 的出版物也会随之更新。该方法提供了一个持续的 NCWF 元素集合。这些元素是稳定的、灵活的以及技术可靠的，可以作为参考资料对从业人员进行培训和教育。

此外，我们也会开发新的参考资料，与 NCWF 元素互相参照。在可能的范围内，数字参考资料也将发布至 NICE 的网站，作为运用 NCWF 的辅助资料和关联资料。

4.1 前瞻性的追加概念

有几个岗位相关的元素已经在多次讨论中浮现出来，但是这些内容目前并没有被整合进 NCWF。这些可能是我们将要进一步研究的领域。未来将要调研的领域是：

- **系统安全工程（SSE）**：系统安全工程（系统工程中的一个特殊工程学科）的许多元素构成了一个完全集成的、系统级的网络空间安全图景。下一步的研究方向将着眼于确保所描述的职责和 KSA，能完全支持 NIST 草案（SP） 800-160 中描述的 SSE 生命周期。系统安全工程——在可信安全系统工程中多学科方法的考虑[15]。SP 800-160 描述了 SSE 如何“帮助确保在系统生命周期中运用了适宜的安全原理、概念、方法和实践，能够从各种形式的不利环境（比如破坏、危险和威胁）中保护资产，达到利益相关方的目标，降低安全脆弱性，从而降低系统对灾害的感染性，提供足够的证据证明系统的可信度已达到预期水平——这种可信度水平，换言之，就是利益相关方共同商定的资产保护期望，即使在诸如此类的不利环境中也能充分地持续不断地得到满足。
- **职务和岗位角色的关系**：职务是员工在组织机构中工作或职位的说明。各组织机构之间的职位各不相同。比起从职务去判断一个工作是否定位在网络空间安全领域，从职责去判定网络空间安全岗位角色，可能更加有效。对于联邦政府来说，开发一个专用的网络空间安全工作体系可以让 NCWF 与职务之间的转换变得更简单。它也将使网络空间安全职位编制和目标人才发展变得更加简单。（例如招聘和激励，培训、挽留等程序）
- **能力素质**：有关能力素质模型的大量工作业已完成，这让 NCWF 参与者在很多方面受用。美国劳工部就业和培训管理局（ETA）[8]给能力素质的一个定义就是“应用或使用知识、技能、能力、行为和个人特长来圆满地履行关键工作任务、特定职能或者胜任给定角色或职位的能力”。 除了列举的这些技术性 KSA，能力素质模型也需要考虑行为指标和非技术指标，比如个人效率、学历和职场竞争力。关于这

些考量的更多信息可以从美国劳工部的 CareerOneStop 网站[4] 获得。

- **精通水平和职业路径：**初学者、中级和高级/专家精通水平可以通过工作经历、认证证书、能力技能和 KSA，以及培训和拓展活动来说明。美国国土安全部 CWDT 有一个被称为“推进、发展你的员工”的章节，包含了创建自定义网络空间安全职业发展路径的模版，相关培训链接，认证证书和专业活动，以及留住各个水平的员工的方法。私人部门、协会和组织机构不妨创建有关精通水平和职业路径的自有出版物。

附录 A-NCWF 元素列表

A.1 NCWF 人才类别

表格 2 对 NCWF 的每一个类别给出了描述。每个类别都包含一个标识符（比如 SP），便于快速引用，也有利于 NCWF 岗位角色标识符的创建。（见表格 4-NCWF 岗位角色）

注释：附录 A 和附录 B 的内容来自多个来源。欢迎反馈关于 NCWF 组件描述（包括职责、KSA）的意见。关于从业者在特定岗位角色可能需要履行的其他职责以及关联的 KSA，作者也诚恳地征求意见。

表格 2 NCWF 人才类别

类别	描述
Securely Provision (SP) 安全基础设施提供	概念化、设计、建造安全的 IT 系统，负责系统和/或网络各个方面的开发
Operate and Maintain (OM) 运营与维护	为 IT 系统高效安全运行提供支持、管理和保障能力。
Oversee and Govern (OV) 监管与治理	提供领导、管理、指导或发展和倡议，让组织机构更有效的进行网络空间安全工作
Protect and Defend (PR) 保护与防御	识别、分析、降低内部 IT 系统和/或网络的威胁
Analyze (AN) 分析	对收到的网络空间安全信息进行高度专业化的审查和评估，以决定情报的价值。
Collect and Operate (CO) 搜集与运作	提供专业化的侦查和欺骗手段，收集可以作为情报的网络空间安全信息。
Investigate (IN) 调查	针对 IT 系统、网络以及数字证据相关的网络空间安全事件和犯罪进行调查。

A.2 NCWF 专业领域

表格 3 提供了 NCWF 每个专业领域的描述。和 NCWF 类别一样，每个专业领域都包含一个标识符（比如 RM），有助于快速引用和进一步引导 NCWF 岗位角色标识符的创建。（见表格 4-NCWF 岗位角色）

表格 3 NCWF 专业领域

类别	专业领域	专业领域描述

Securely Provision 安全基础设施提供(SP)	Risk Management (RM) 风险管控	监督、评价、协助文档编写，验证、评估、以及必要的授权处理，确保已有的和新的 IT 系统满足组织机构网络空间安全和风险管控需求。从内部和外部角度，确保采取合适的风险处理、合规性和保障性措施。
	Software Development (DEV) 软件开发	遵循软件保障的最佳实践，开发和编写/编码新的（或修改现有的）计算机应用、软件或专门的实用程序。
	Systems Architecture (ARC) 系统架构	设计系统概念，在系统开发生命周期的能力阶段工作，将技术和环境条件（比如法律和法规）融入到系统和安全的设计与过程中。
	Technology R&D (RD) 技术研发	进行技术评估和集成处理，提供和支持原型能力和/或效用评估
	Systems Requirements Planning (RP) 系统需求规划	与客户沟通收集和评估功能需求，并将其翻译为技术解决方案，对客户提供信息系统适用性指导，帮助其满足业务需求。
	Test and Evaluation (TE) 测试评估	开发并组织系统测试，通过运用高效益的原则和方法，规划、评估、检验、验证系统或 IT 系统要素的技术、功能和性能特点（包括互操作性），评估（软件）规格和需求的一致性。
	Systems Development (SYS) 系统开发	在系统开发生命周期的开发阶段工作。
Operate and Maintain (OM) 运营与维护	Data Administration (DA) 数据管理	开发和管理用于存储、查询和调用数据的数据库和/或数据管理系统。
	Knowledge Management (KM) 知识管理	管理和执行进程和工具，这些进程和工具让组织机构可以识别、记录并访问智力资本和信息内容。
	Customer Service and Technical Support (TS) 客户服务和技术支持	解决问题、安装、配置、排解故障、应客户需求和问询（比如分层级的客户支持），提供维护和培训支持。
	Network Services (NET)	安装、配置、测试、操作、维护和管理网络以及它们的防火墙，包括硬件（比如 Hub、网桥、交换机、多路

	网络服务	复用器、路由器、光纤、代理服务和保护式分配器系统）和那些允许共享和传输全频谱信息的软件，以保障信息和信息系统安全。
	Systems Administration (SA) 系统管理	安装、配置、排解故障和维护服务的配置（硬件和软件），确保他们的机密性、完整性和可用性。同时，管理账户、防火墙和（系统）补丁。负责（系统的）访问控制、口令、账号创建和管理。
	Systems Analysis (AN) 系统分析	主导实施系统安全的集成/测试、操作和维护。
Oversee and Govern (OV) 监管与治理	Legal Advice and Advocacy (LG) 法律咨询和辩护	在各种相关领域，向管理层和职工提供法律范围内的切实忠告和中肯建议。普及法律知识和政策变化，通过大量的书面和口头工作（包括法律文件和诉讼），为委托人进行主张、辩护。
	Training, Education, and Awareness (ED) 培训、教育和养成	组织实施相关领域的人员培训，开发、计划、协调、交付和/或评估合适的培训课程、方法，及技术。
	Cybersecurity Management (MG) 网络空间安全管理	监管信息系统或网络的网络空间安全程序，应对处理组织机构内、特定项目内或其他职责范围内的信息安全隐患，包括策略、人员、基础设施、需求、政策实施、应急预案、安全意识以及其他资源。
	Strategic Planning and Policy (PL) 战略规划和策略	制定策略、规划，并 / 或主动调整政策，以配合组织机构的网络空间安全举措或形势所需的变更 / 提升。
	Executive Cybersecurity Leadership (EX) 网络空间安全执行领导	监督、管理和/或领导网络空间安全工作和相关员工。
	Acquisition and Program/Project Management (PM) 采购和项目管理	运用数据知识、信息，流程、组织机构影响力，技能和专业知识，以及系统、网络和信息交换能力来管理采购项目。负责统筹硬件、软件和信息系统的采购项目，以及其他项目管理策略。对使用信息技术（包括国家安全系统）的采购项目，提供直接支持，在整个采办项目的寿命周期中，贯彻 IT 相关法律和政策，提供 IT 相关的指导。
Protect and Defend (PR) 保护与防御	Cybersecurity Defense Analysis (DA) 网络空间安全防御分析	使用防御手段和从多个来源收集到的信息，来识别、分析和报告网络内正在发生或可能发生的事件，以保护信息、信息系统和网络免受侵害。

	Cybersecurity Defense Infrastructure Support (INF) 网络空间安全防御基础设施支持	测试、实施、部署、维护、审查和管理硬件和软件基础设施。这些基础设施是有效管理计算机网络防御服务提供者网络和资源必须具备的。监控网络主动纠正未授权的行为。
	Incident Response (IR) 事件响应	应对相关领域的危机或紧急情况，缓解当前或潜在的威胁。根据需要使用减灾、预备方案、响应和恢复方法，最大化挽救系统寿命、保护资产和信息安全。保护财产和信息安全。对相关的响应行为进行调查分析。
	Vulnerability Assessment and Management (VA) 漏洞评估和管理	对威胁和漏洞进行评估，确定是否与可容配置存在偏差，是否偏离企业或当地政策导向，评估风险等级，在可操作和非操作环境下开发和/或推荐合适的应对措施。
Analyze (AN) 分析	Threat Analysis (TA) 威胁分析	对网络空间安全犯罪或外国情报机构的能力和活动进行识别和评估。形成成果帮助引导和支持执法部门和反情报调查活动。
	Exploitation Analysis (XA) 渗透分析	分析收集的信息，识别漏洞和潜在的渗透利用。
	All-Source Analysis (AN) 全源分析	分析多个来源，多个标准和多个情报社区的威胁情报。在具体上下文环境中综合分析和处理情报，洞察情报中可能蕴含的暗示。
	Targets (TD) 目标分析	应用一个或多个区域、国家、非政府组织和/或技术的前沿知识
	Language Analysis (LA) 语言分析	应用语言、文化和专业技术，来支持信息采集、分析和其他网络空间安全活动。
Collect and Operate (CO) 搜集与运作	Collection Operations (CL) 搜集与运作	通过适当的策略，遵循在搜集管理流程下建立的优先级进行信息搜集
	Cyber Operational Planning (PL) 网络空间运营规划	深入贯彻联合目标和网络空间安全规划进程。收集信息、制定详细运营计划和命令以满足需求。构建战略性和业务层面的规划，覆盖集成化信息和网络空间运营的全业务范围。
	Cyber Operations (OP) 网络空间运营	为收集网络犯罪或国外情报机构的证据信息从事各种活动，以减少可能的或实时的网络威胁，防范间谍或内部威胁，外部破坏，国际恐怖主义活动，或支持其他情报活动。
Investigate (IN) 调查	Cyber Investigation (CI) 网络空间调查	使用战术、技术和程序手段，涵盖全方位的调查工具和工序。包括但不限于面谈和审讯技术，监听和反监听，监听检测，适当平衡各方利益，规避情报收集工作的诉讼风险。

	Digital Forensics (FO) 数字取证	收集、处理、保存、分析和呈现计算机相关的证据，以支持网络漏洞防治，和/或有关（计算机）犯罪、诈骗以及反情报机构或执法部门的调查

A.3 NCWF 岗位角色

表格 4 提供了 NCWF 中每个岗位角色的描述。每个岗位角色通过类别和专业领域再加一个序列号来识别。（比如 SP-RM-001 是 SP 这个类别、RM 这个专业领域的第一个岗位角色。）一些岗位角色的描述来源于外部文档（比如国家安全系统指令委员会 CNSSI 4009）。这些来源信息被列入“描述”栏中。如第四部分所述，NCWF 将会定期的更新这个表格。某些岗位角色可能被弃用、被增加、或被修改，以反映网络空间安全人才前景的变化。

表格 4 NCWF 岗位角色

类别	专业领域	Work Role 岗位角色	NCWF ID	岗位角色描述
Securely Provision (SP) 安全基础设施提供	Risk Management (RM) 风险管控	授权官员/指定代表	SP-RM-001	获得授权的高级官员或主管将正式承担责任，在对组织机构运营、组织机构资产、个人、其他组织机构和国家而言的合理风险范围内，进行信息系统的运营工作 (CNSSI 4009).
		安全控制评估师	SP-RM-002	对管理、运营、技术安全控制和内置的或从某个 IT 系统继承的控制增强装置，进行独立的、综合的评估，以确定安全控制的整体有效性。
	Software Development (DEV) 软件开发	软件开发者	SP-DEV-001	开发、创建、维护、编写/编码 新的（或修改现有的）计算机应用、软件或专门的实用程序。
		安全软件评估师	SP-DEV-002	对新的或现有的计算机应用、软件或专门的实用程序进行安全分析并提供可操作的结果
	Systems Architecture (ARC) 系统架构	企业架构师	SP-ARC-001	开发并维护业务、系统和信息处理过程，支持企业使命目标。开发符合基准和目标架构的信息技术规则和需求。
		安全架构师	SP-ARC-002	规划企业和系统安全，贯穿整个开发生命周期，将技术和环境条件（比如法律和法规）融入到安全的设计与过程中。
	Technology R&D (RD) 技术研发	研发专家	SP-RD-001	研究软件系统，以开发新功能，确保与网络空间安全完全集成。进行综合广泛的技术研究来评估网络空间系统中的潜在漏洞。
	Systems Requirements Planning (RP) 系统需求规划	系统需求规划师	SP-RP-001	与客户协商评估功能需求，并将功能需求转化为技术解决方案。
	Test and Evaluation (TE) 测试评估	系统测试和评估专家	SP-TE-001	计划、准备和执行系统测试，对照（系统）规格和需求评估测试结果，分析/汇报测试结果。
	Systems Development	信息系统安全开发	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的安全性。

	(SYS) 系统开发	者		
		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。
Operate and Maintain (OM) 运营与维护	Data Administration (DA) 数据管理	数据库管理员	OM-DA-001	管理用于存储、查询和调用数据的数据库和/或数据管理系统。
		数据分析	OM-DA-002	对多个不同来源的数据进行检查分析，以发现新的洞见。针对用于数据建模、数据挖掘以及数据研究的复杂的、企业级规模的数据集，设计并实现自定义算法、流程和布局。
	Knowledge Management (KM) 知识管理	知识管理管理者	OM-KM-001	负责管理和运营（知识管理）的流程和工具。这些过程和工具可以让组织机构可以识别、记录和访问智力资本和信息内容。
	Customer Service and Technical Support (TS) 客户服务和技术支持	技术支持专家	OM-TS-001	利用客户级的硬件和软件，对需要帮助的客户提供技术支持，严格遵循已有的或已批准的组织机构流程组件（如主机事件管理计划，如适用时）。
	Network Services (NET) 网络服务	网络运营专家	OM-NET-001	对包括硬件和虚拟环境在内的网络服务/系统，进行计划、实施和运营。
	Systems Administration (SA) 系统管理	系统管理员	OM-SA-001	对硬件和软件进行安装、配置、故障解决和维护，管理系统账号。
	Systems Analysis (AN) 系统分析	系统安全分析师	OM-AN-001	负责对系统安全集成、测试、运行和维护进行分析和开发。
Oversee and Govern (OV) 监管与治理	Legal Advice and Advocacy (LG) 法律咨询和辩护	网络空间法律顾问	OV-LG-001	对网络空间相关法律话题，提供专业的法律意见和建议。
		隐私合规管理者	OV-LG-002	督促、监管隐私合规项目以及隐私项目工作人员，帮助安全工作人员和他们团队的满足隐私合规要求。
	Training, Education, and Awareness (ED) 培训、教育和养成	网络空间教程开发者	OV-ED-001	根据教学计划需求，开发、规划、协调和评估网络空间培训/教育课程、方法和技术。
		网络空间讲师	OV-ED-002	制定和实施网络空间领域从业人员的培训或教学。
	Cybersecurity Management (MG)	信息系统安全管理者	OV-MG-001	负责一个程序、组织机构、系统或飞地的网络空间安全。

	网络空间安全管理	通信安全管理者	OV-MG-002	管理一个组织机构的通信安全资源（CNSSI 4009）
	Strategic Planning and Policy (PL) 战略规划和策略	网络空间人力开发者和管理者	OV-PL-001	制定网络空间人才规划、战略和指南，以支持网络空间人才的人力、人才、培训和教育需求，应网络空间政策、条款、材料、人员结构、以及教育和培训需求而变化。
		网络空间策略和战略规划师	OV-PL-002	制定网络空间规划、战略和政策，与组织机构网络空间的使命和宗旨相符。
	Executive Cyber(security) Leadership (EX) 网络空间安全执行领导	网络空间安全执行领导	OV-EX-001	制定权威决策，建立组织机构网络空间和网络空间相关资源和/或业务的愿景和方向。
	Acquisition and Program/Project Management (PM) 采购和项目管理	项目管理者	OV-PM-001	领导、协调、沟通、整合，并对项目的全面成功负责，确保符合关键代理优先级。
		IT项目管理者	OV-PM-002	直接管理IT项目，提供独特的服务或者产品。
		产品支持管理者	OV-PM-003	管理现场支持所需的功能包，保持系统和组件的就绪状态和业务能力。
		IT投资和投资组合管理者	OV-PM-004	掌管IT能力的投资组合，使其符合企业使命的总体要求和组织机构优先事项。
		IT项目审计	OV-PM-005	对IT项目或它的单独组件进行评估，确保它们符合已发布的标准。
Protect and Defend (PR) 保护和防御	Cyber Defense Analysis (DA) 网络空间安全防御分析	网络空间安全防御分析师	PR-DA-001	使用从自多个网络防御工具（比如IDS告警、防火墙、网络流量日志）收集而来的数据，研究分析这些环境中发生的事件，从而抑制安全威胁。
	Cyber Defense Infrastructure Support (INF) 网络空间安全防御基础设施支持	网络空间安全防御基础设施支持专家	PR-INF-001	测试、实施、部署、维护和管理硬件和软件基础设施。
	Incident Response (IR) 事件响应	网络空间防御事件响应员	PR-IR-001	针对网络环境或飞地内的网络事件进行调查、分析和响应。
	Vulnerability Assessment and Management (VA) 漏洞评估和管理	漏洞评估分析师	PR-VA-001	在网络环境或飞地中对系统和网络进行评估，找出哪些系统/网络偏离了合理配置、飞地政策或本地政策。评测应对已知漏洞的纵深防御架构的有效性。
Anal	Threat Analysis	预警分析	AN-TA-0	开发独特的网络空间指标，以保持在高动态运

yze (AN) 分析	(TA) 威胁分析	师	01	行环境下对（系统）运行状态的持续感知。收集、处理、分析并传达网络告警评估（信息）。
	Exploitation Analysis (XA) 渗透分析	渗透分析师	AN-XA-001	通过协作，找出获取信息和搜集信息的空白区，通过网络采集和/或准备活动来填补空白。利用所有授权资源和分析技术渗透目标网络。
	All-Source Analysis (AN) 全源分析	全源分析师	AN-AN-001	分析来自一个或多个来源的数据/信息，创建准备环境，响应信息请求，并提交情报收集和生产要求，支持规划和运营
		任务评估专家	AN-AN-002	制定绩效考核计划和措施。对网络活动进行必要的战略层面和运营层面的效果评估。确定系统是否按照预期运行，为运行效能的测定提供建议。
	Targets (TD) 目标分析	目标开发人员	AN-TD-001	执行目标系统分析，构建和/或维护电子目标文件夹，该文件夹包括了从环境准备、和/或内部或外部情报来源的所有情况。协调合作伙伴的目标活动和情报机构，提出备选目标进行审查和验证。
		目标网络分析师	AN-TD-002	对收集的和开源的数据进行高级分析，确保目标连续性，为目标及其活动进行画像，开发技术以获取更多的目标信息。基于对目标技术、数字网络和网络上的应用程序的了解，确定目标是如何进行通信、移动、操作和生存的。
	Language Analysis (LA) 语言分析	多学科语言分析师	AN-LA-001	运用目标/威胁相关的语言和文化专业知识和技术知识来处理，分析和/或传达来自语言，语音和/或图像材料的情报信息。创建和维护特定语言的数据库和工作辅助工具，以支持网络行动的执行，并确保关键知识的共享。在外语密集型或跨学科型项目中，提供相关的专业知识。
Collect and Operate (CO) 搜集与运作	Collection Operations (CL) 搜集与运作	全源搜集管理者	CO-CL-001	确定搜集机构和环境；将优先信息需求纳入收集管理；开发（相关）概念以支撑领导意图。确定可用的搜集资产能力，标识新的搜集功能，并构建和传播搜集计划。监控已委派的搜集任务的执行，确保搜集计划的高效执行。
		全源搜集需求管理者	CO-CL-002	使用现有的资源和方法，评估搜集运行情况，开发基于效果的搜集需求策略，提高搜集（效果）。开发、处理、验证和协调搜集需求的提交。评估搜集资产和搜集运营的表现。
	Cyber Operational Planning (PL) 网络空间运营规划	网络空间情报规划师	CO-PL-001	制定详细的情报计划，以满足网络空间运营需求。协助网络空间运营规划师，识别、验证和征集搜集与分析的需求。参与网络行动的目标选择、验证、同步和执行。同步情报活动，以支持组织机构在网络空间的目标。
		网络空间	CO-PL-0	通过与其他规划师，运营人员和/或分析师协

		运营规划师	02	作，制定详细的计划，以引导或提示网络空间运营的合适范围。参与目标选择，验证，同步，并且在网络行动执行过程中实现集成。
		合作伙伴集成规划师	CO-PL-003	推进跨组织或跨国界的网络合作伙伴之间的合作。通过提供指导，资源和协作，支援合作伙伴网络团队的整合，发挥最佳实践并促进组织机构在联动的网络行动中实现目标。
	Cyber Operations (OP) 网络空间运营	网络空间运营专员	CO-OP-001	进行搜集、处理和/或地理定位，来渗透、定位和/或跟踪感兴趣的目标。进行网络导航、战术取证分析，并依据指示，执行线上操作。
Investigate (IN) 调查	Cyber Investigation (CI)网络调查	网络空间犯罪调查专员	IN-CI-001	采用可控的、有据可依的分析调查技术，对证据进行识别、收集、检查和保存。
	Digital Forensics (FO) 数字取证	取证分析师	IN-FO-001	对基于计算机的犯罪进行深度调查，包括与网络入侵事件相关的数字介质和日志。 针对基于计算机的犯罪进行深度调查，建立文档证据或物证，包括与网络入侵事件相关的数媒文件和日志。
		网络空间防御取证分析师	IN-FO-002	分析数字证据，调查计算机安全事件，以获取有用的信息，消除系统/网络安全隐患。

A.4 NCWF 岗位职责

表格 5 提供了与 NCWF 岗位角色相关联的各种职责列表。由于这些职责已经久经演化，并且将继续演化下去，所以并没有以特定的标准排序，而将以简单的方式按序号添加。

表格 5 NCWF 岗位角色任务

Task	职责描述
T0001	获取和管理必要的资源，包括领导支持，财务资源，关键的安全人员，以支撑信息技术（IT）安全目标，降低整个组织风险。
T0002	获取必要的资源，包括财务资源，组织开展有效的企业持续经营计划。
T0003	与高级管理人员如首席信息官（CIO）商量风险水平和安全态势。
T0004	与高级管理人员如 CIO 讨论信息安全程序的成本/效益分析、政策、流程以及制度和元素。
T0005	向相关高层或授权人告知组织机构的网络空间安全态势变化的影响。
T0006	支持组织机构在法律和法律程序中的官方立场。
T0007	对数据需求和规范进行分析和定义。
T0008	为数据容量要求的预期变化做分析和规划。
T0009	分析信息以判断、建议、并计划开发新的应用程序或改进现有的应用程序。
T0010	分析组织机构的网络防御政策和配置，以评估对法规和组织指令的遵守。
T0011	分析用户需求和软件要求，以确定在时间和成本约束下设计的可行性。
T0012	分析设计限制条件，分析权衡、详细的系统以及安全设计，并考虑生命周期支持。

T0013	使用编码和测试标准，使用安全测试工具包括“fuzzing”静态分析代码扫描工具，并进行代码审查。
T0014	使用安全代码文档。
T0015	将安全策略应用到相互接口的应用程序中，例如组织机构对组织机构（B2B）的应用。
T0016	运用安全性策略以满足系统的安全目标。
T0017	运用以服务为导向的安全结构原理，满足组织机构的机密性、完整性和可用性要求。
T0018	评估系统所使用的网络空间安全措施的有效性。
T0019	评估计算机系统的威胁和漏洞，开发安全风险配置文件。
T0020	开发网络防御工具。
T0021	使用工作模型或理论模型构建、测试和修改产品原型。
T0022	在需求阶段捕捉使用的安全控件，整合过程内的安全，识别关键安全目标，并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进度的干扰。
T0023	描述和分析网络流量以识别网络资源的异常活动和潜在威胁。
T0024	收集并维护满足系统网络空间安全报告所需的数据。
T0025	在各级组织机构利益相关者中沟通信息技术（IT）安全的价值。
T0026	编译和编写程序开发文档以及后续版本，在编码指令中插入注释，以便其他人能够理解程序。
T0027	对日志文件、证据和其他信息进行分析，以确定识别对网络入侵者的最佳方法。
T0028	进行和/或支持对网络资产的授权渗透测试。
T0029	进行功能和连接测试，确保持续的可操作性。
T0030	开展互动培训，营造有效的学习环境。
T0031	对受害人和目击者进行采访，采访、审讯犯罪嫌疑人。
T0032	为了适当的安全控制，对应用程序的安全设计进行隐私影响评估（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，开发，记录和完善功能需求和规格。
T0034	与系统分析员、工程师、程序员和其他人协商设计应用程序，并获取有关项目局限性、能力、性能要求和接口的信息。
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、通道）。
T0036	尽可能的通过动态分析识别入侵，确认已知的入侵并发现新的信息。
T0037	构建访问路径的信息套件（例如，链接页），以方便终端用户的访问。
T0038	开发基于客户访谈和需求的威胁模型。
T0039	与客户协商评估功能需求。
T0040	与工程人员协商评估硬件和软件之间的接口。
T0041	对企业范围内的网络空间防御技术员协调提供专家技术支持，以解决网络空间防御事件。
T0042	协调网络空间防御分析师，管理和监督规则和签名的更新（例如，入侵检测/防护系统、防病毒、内容黑名单）以便运行专业的网络空间防御应用。
T0043	协调企业范围内的网络空间防御人员验证网络警报。
T0044	与利益相关者合作，建立关于项目运营、战略、使命保障的企业持续运营计划。
T0045	根据需要协调系统架构师和开发人员，为设计解决方案的开发提供监督。
T0046	通过适当的改变和复核程序，确保产生预期的结果。

T0047	关联事件数据确认具体的漏洞并提出建议，便于迅速修复。
T0048	创建一个可靠的、重复的证据取证（即法医图像），确保原始证据不会被无意修改，用于数据的恢复和分析过程。包括但不限于硬盘、软盘、光盘、掌上电脑、手机、GPS、和所有的磁带格式文件。
T0049	利用技术手段解密被抓数据。
T0050	定义并区分在灾难性故障后，需要恢复的基本系统功能或业务功能的优先级。
T0051	基于关键系统功能，定义是适当的系统可用性水平，确保系统需求符合适当的灾难恢复和连续性运行的需求，包括系统恢复/重建所需的任意适当的故障切换/备份站点、备份、物质保障。
T0052	根据客户需求定义项目范围和目标。
T0053	设计和开发网络空间安全或网络空间安全功能的产品。
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，以充分解决网络空间安全的要求。
T0056	设计或集成适当的数据备份功能到整个系统设计中，确保对于备份数据的安全系统备份和受保护的存储，存在适当的技术和程序流程。
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	根据测试结果确保开发能力的水平。
T0059	制定一项利用电脑和互联网调查涉嫌犯罪、违规或可疑活动的计划。
T0060	开发了解信息终端用户的需求和要求。
T0061	开发和指导系统测试、验证程序和文件。
T0062	制定和记录设计程序和流程的要求、能力和限制。
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库存程序，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架构或系统组件。
T0068	制定数据标准、政策和程序。
T0069	为组件和接口规范开发详细的安全设计文档，支持系统设计和开发。
T0070	为开发中的系统研制灾难恢复和连续性操作计划，并确保在进入生产环境之前完成测试。
T0071	开发/集成系统和网络的多级安全要求或主要适用于政府组织处理多个级别（例如，公开，秘密，机密）分类数据的要求。
T0072	开发风险监控，遵守和保证努力的方法。
T0073	开发新的或识别现有的意识和培训材料，适应目标受众。
T0074	制定政策、方案和实施指南。
T0075	根据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，并根据需要推荐系统或系统组件的安全更改。
T0077	开发安全代码和错误处理。
T0078	为系统和/或应用程序开发特定的网络空间安全对策和风险缓解策略。
T0079	制定规范保证风险，合规性，并保证工作符合安全性、弹性和可靠性要求的软件系统，体系和网络环境。
T0080	制定测试计划，以满足规格和要求。

T0081	判断网络连接问题。
T0082	在整个搜集周期记录和处理组织机构的信息安全、网络空间安全架构和系统安全工程要求。
T0083	起草系统操作初级或剩余的安全风险报告。
T0084	采用安全配置管理流程。
T0085	确保所有系统的安全运行和维护活动得到适当的记录和更新。
T0086	确保商业产品的安全补丁整合到系统的设计中，并符合管理层根据预期的操作环境拟定的时间线。
T0087	确保所有数字介质监管链与《联邦证据规则》一致。
T0088	确保网络空间安全功能产品或其他补偿安全控制技术将识别风险降到可接受的水平。
T0089	确保安全改进措施已按需评估、验证和实施。
T0090	确保获得或开发的系统和架构与组织机构的网络空间安全架构准则相一致。
T0091	确保网络空间安全检查，测试和审查的网络环境相互协调。
T0092	确保系统或组织机构的连续性计划与网络空间安全要求一致。
T0093	确保使用 IS 安全工程方法获得保护和检测能力，并符合组织级的网络空间安全架构。
T0094	与利益相关者建立和维护沟通渠道。
T0095	基于组织机构的整体安全策略全面建立组织机构信息安全体系架构（EISA）。
T0096	适时建立事件响应团队和其他组织的关系，包括内部组织（如法律部门）和外部组织（如执法机构、供应商和公关人员）。
T0097	评估和批准开发工作以确保基线安全措施得到适当的安装。
T0098	评估合同，以确保符合资金，法律和程序要求。
T0099	在决策过程中评估成本效益、经济和风险分析。
T00100	评估诸如报告格式要求、成本约束、安全限制需求等因素确定硬件配置。
T00101	评估现有培训项目的有效性和综合性。
T00102	评估法律、法规、政策、标准或程序的效力。
T00103	检查恢复数据的信息关联性以应对手头的问题。
T00104	融合计算机网络攻击分析与犯罪和反情报调查行动。
T00105	确定组件或元素，将安全功能分配给这些元素，并描述元素之间的关系。
T00106	识别替代信息安全策略，以解决组织机构的安全目标。
T00107	在新系统的测试和实施过程中识别和指导技术问题的修复（如：识别与发现针对不可互操性的通信协议的应急措施）
T00108	与组织机构利益相关者合作对关键业务职能进行确定和优先排序。
T00109	根据系统的连续性和可用性要求，识别并优先考虑必要的系统功能或子系统以支持系统恢复或恢复后的基本功能或业务功能。
T00110	识别和确定一个安全事件是否是违反法律而需要具体的法律诉讼。
T00111	在更高层次上识别基本常见的编码缺陷。
T00112	确定数据或情报的证据价值，以支持反间谍和刑事调查。
T00113	识别数字证据的检查和分析的方式，以避免无意改变。
T00114	确定犯罪证据的要素。
T00115	确定新技术或技术升级的信息技术安全程序影响。
T00116	确定组织机构政策利益相关者。

T00117	确定企业计算机系统的安全影响，并在系统的软件开发中，运用中心化和非中心化环境方法论。
T00118	识别稳态运行和管理软件的安全问题，和在产品生命期结束时需采取的安全措施。
T00119	识别、评估、推荐系统使用的网络空间安全或网络空间安全功能产品，并确保推荐的产品符合组织机构的评估和验证要求。
T00120	识别，收集，并抓住文件或物理证据，包括数字媒体和与网络入侵事件，调查和操作相关的日志。
T00121	执行新的系统设计程序，测试程序和质量标准。
T00122	为新的或现有系统实施安全设计。
T00123	为系统或应用程序实施具体的网络空间安全措施。
T00124	将网络空间安全漏洞解决方案纳入系统设计（例如，网络空间安全漏洞警报）。
T00125	安装和维护网络基础设施设备中的操作系统软件（例如，iOS 固件）。
T00126	安装或更换网络集线器、路由器和交换机。
T00127	整合和调整信息安全和/或网络空间安全政策，以确保系统分析符合安全要求。
T00128	集成自动化功能，用于更新或修补实用系统软件，基于当前或预计的补丁时限要求的操作环境系统开发流程和程序，手动更新和修补系统软件。
T00129	将新系统集成到现有的网络架构中。
T00130	与外部组织机构（如公共事务，执法，指挥或部件检查员）保持联系，以确保适当和准确地传播事件和其他计算机网络防御信息。
T00131	应用法律、法规、政策、标准或程序来解释具体问题。
T00132	解释或核准关于新信息技术能力的安全要求。
T00133	解释违规模式，以确定其对企业的网络空间安全计划的风险和/或整体效益水平的影响。
T00134	基于安全策略引导和调整信息技术的优先安全项。
T00135	领导和监督信息安全预算，人员编制和合同。
T00136	根据组织机构的政策维护基线系统安全。
T00137	维护数据库管理系统软件。
T00138	维护部署的网络空间防御审计工具包（例如，专门的网络空间防御软件和硬件），以支持网络空间防御审计任务。
T00139	维护目录复制服务，通过优化路由使信息从后端服务器自动向前单元复制。
T00140	通过发布、订阅和警报功能保持信息交流，使用户能够根据需要发送和接收关键信息。
T00141	信息系统安全保障和坚定材料维护。
T00142	维护与网络空间防御审计相关的适用网络防御政策、法规和合规性文件的知识。
T00143	根据测试结果提出建议。
T00144	管理帐户，网络权利，有权使用系统和设备。
T00145	管理和核准认可的包（例如，ISO / IEC 15026-2）。
T00146	管理数据的编译、编目、缓存、分发和检索。
T00147	管理信息安全数据源的监控，以保持组织机构的态势感知。
T00148	管理针对企业范围的计算机网络防御指导（如，TCNOs，运营理念，网络分析师报告，NTSM，MTOs）
T00149	对企业内部网络空间威胁防御信息和产品，进行威胁分析管理或目标分析管理

T00150	遵照信息技术（IT）安全性，应变能力和可靠性要求监控和评估系统的合规性。
T00151	监控和评估该企业的网络空间安全保障措施的有效性，以确保他们提供预期的保护水平。
T00152	监控和维护数据库以确保最佳性能。
T00153	监控网络容量和性能。
T00154	监控和报告知识管理资产和资源的使用情况。
T00155	对可能对环境造成持续和立即影响的事件进行记录和升级处理（包括事件的历史，状况和对进一步行动的潜在影响）
T00156	监督并对配置管理提出建议。
T00157	监督信息安全培训和意识计划。
T00158	参与安全评估和授权过程中的信息安全风险评估。
T00159	参与开发或修改计算机环境网络空间安全计划的方案和要求。
T00160	修补网络漏洞，确保信息的对外保护。
T00161	执行日志文件的分析，从各种来源（例如，个别主机日志，网络流量日志，防火墙日志和入侵检测系统[IDS]日志），以确定可能对网络安全的威胁。
T00162	执行备份和恢复数据库，以确保数据完整性。
T00163	执行网络空间防御事件分类，包括确定范围、紧迫性、和潜在的影响；识别特定的脆弱性；并提出建议，使快速修复。
T00164	进行网络空间防御趋势分析和报告。
T00165	执行动态分析，启动一个驱动器的“图像”（不必有原驱动器），在本机环境查看用户可能已经看到的入侵。
T00166	对企业内部各种来源收集的信息执行事件相关性，以获得态势感知，并确定所观察到的攻击的有效性。
T00167	执行文件签名分析。
T00168	对已建立的数据库执行哈希比较。
T00169	对开发的应用程序和/或系统进行网络空间安全测试。
T00170	在企业系统的进行初始的可靠的图像证据搜集，检查得出可行的缓解/修复措施。
T00171	执行安全功能和弹性攻击的综合质量保证测试。
T00172	执行实时取证分析（例如，将 Helix 与 LiveView 结合使用）。
T00173	执行时间轴分析。
T00174	执行需求分析，以确定新的和改进的业务流程解决方案机会。
T00175	执行实时网络空间防御事件处理（例如，法庭收集，入侵相关和跟踪，威胁分析和直接系统补救）任务，以支持可部署的事件响应小组（IRT）。
T00176	执行安全编程和识别代码中的潜在缺陷以减少漏洞。
T00177	执行安全审查，识别安全架构中的差距，并制定安全风险管理计划。
T00178	执行安全审查并确定安全架构中的安全漏洞，为纳入风险缓解战略提出建议。
T00179	执行静态媒介分析。
T00180	在专门的网络空间防御应用和系统（例如，防病毒，审计和修复）或虚拟专用网络（VPN）设备上执行系统管理，包括安装，配置，维护，备份和恢复。
T00181	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，漏洞和事件概率）。
T00182	执行第 1，2，和 3 层恶意软件分析。

T00183	执行验证步骤，将实际结果与预期结果进行比较，分析差异，识别影响和风险。
T00184	为系统和网络的初始安装计划进行安全授权评审和保证案例开发。
T00185	计划和管理知识管理项目的交付。
T00186	计划，执行和验证数据冗余和系统恢复程序。
T00187	根据练习结果或系统环境计划和建议修改或调整。
T00188	准备确定技术和程序结果的审计报告，并提供建议补救策略/解决方案。
T00189	准备描述输入，输出和逻辑操作的详细工作流图表和图解，并将它们转换为以计算机语言编码的一系列指令。
T00190	通过确保数据完整性来准备用于成像的数字介质（例如，根据标准操作程序写拦截器）。
T00191	准备用例来证明对特定信息技术（IT）解决方案的需求。
T00192	准备，分发和维护有关网络系统操作安全的计划，指令，指导和标准操作程序。
T00193	审核犯罪现场。
T00194	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。
T00195	根据任务要求提供管理的相关信息流（通过网络门户或其他方式）。
T00196	提供有关项目成本，设计概念或设计变更的建议。
T00197	提供对软件应用程序，系统或网络的准确技术评估，记录安全状态，功能和漏洞以及相关的网络空间安全合规性。
T00198	提供与网络空间防御做法相关的网络事件和活动的每日总结报告。
T00199	为开发运营计划的连续性提供企业网络空间安全和供应链风险管理指南。
T00200	提供有关网络要求的反馈，包括网络架构和基础设施。
T00201	为客户或安装团队提供实施开发系统的指南。
T00202	为领导提供网络空间安全指导。
T00203	提供关于安全要求的输入，以包括在工作声明和其他适当的采购文件中。
T00204	为实施计划和标准操作程序提供投入。
T00205	为风险管理框架过程活动提供投入和相关文档（例如，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）。
T00206	通过确保向与其职责相称的业务人员提供网络空间安全意识，基础，识字和培训，为信息技术（IT）人员提供领导和指导。
T00207	提供持续的优化和解决问题的支持。
T00208	提供可能的改进和升级的建议。
T00209	提供关于数据结构和数据库的建议，以确保正确和高质量地生成报告/管理信息。
T00210	提供关于新数据库技术和架构的建议。
T00211	提供系统相关的网络空间安全要求输入，以包括在工作说明书和其他适当的采购文件中。
T00212	向有关人员提供有关数字证据事项的技术援助。
T00213	向上级总部提供技术文件，事故报告，计算机检查结果，摘要和其他情境意识信息。
T00214	接收和分析企业内各种来源的网络警报，并确定此类警报的可能原因。
T00215	识别可能的安全违规，并根据需要采取适当的措施报告事件。
T00216	识别并准确地报告指示特定操作系统的取证工件。
T00217	解决软件接受阶段的安全影响，包括完成标准，风险接受和文档，通用标准和

	独立测试方法。
T00218	根据审查结果推荐新的或修订的安全性，恢复力和可靠性措施。
T00219	推荐安全运行和维护组织机构的网络空间安全所需的资源配置。
T00220	解决法律，法规，政策，标准和程序中的冲突。
T00221	审查授权和保证文件，以确认每个软件应用程序，系统和网络的风险级别在可接受的限制内。
T00222	与利益相关者审查现有和拟议的政策。
T00223	审查或进行信息技术（IT）计划和项目的审计。
T00224	审查培训文件（例如课程内容文件[CCD]，课程计划，学生文本，考试，指导计划书[SOI]和课程说明）。
T00225	保护电子设备或信息源。
T00226	服务于代理和机构间政策委员会。
T00227	推荐政策并协调审查和批准。
T00228	存储，检索和操作数据以分析系统功能和要求。
T00229	发现网络空间安全事件或漏洞时，监督或管理保护或纠正措施。
T00230	支持练习场景的设计和执行。
T00231	为安全/认证测试和评估活动提供支持。
T00232	测试和维护网络基础设施，包括软件和硬件设备。
T00233	跟踪和记录从初始检测到最终解决的网络防御事故。
T00234	跟踪审计结果和建议，以确保采取适当的缓解行动。
T00235	功能需求转化为技术解决方案。
T00236	将安全要求转换为应用程序设计元素，包括记录软件攻击面的元素，进行威胁建模以及定义任何特定的安全标准。
T00237	排除系统硬件和软件故障。
T00238	使用数据雕刻技术（例如，取证工具包 [FTK]，Foremost）提取数据。
T00239	使用联邦和组织机构特定的已发布文档来管理其计算环境系统的操作。
T00240	使用网络监控工具捕获和分析与恶意活动相关的网络流量。
T00241	使用专门的设备和技术来编目，记录，提取，收集，包装和保存数字证据。
T00242	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。
T00243	验证和更新反映应用程序/系统安全设计功能的安全文档。
T00244	对应用软件/网络/系统安全态势按照规定执行的文档偏差进行验证，并建议采取必要的措施来纠正这些偏差。
T00245	验证软件应用/网络/系统的认证和保证文档是最新的。
T00246	撰写和发布网络防御技术，指导，并向适当的用户报告事件结果。
T00247	撰写教学材料（例如标准操作程序，生产手册），为劳动力的相关部分提供详细指导。
T00248	提高管理层对安全问题的认识，确保健全的安全原则反映在组织机构的愿景和目标中。
T00249	研究当前技术以了解所需系统或网络的能力。
T00250	根据任务要求确定定制硬件和软件开发的网络能力战略。
T00251	为外部服务（例如云服务提供商，数据中心）制定安全合规流程和/或审计。
T00252	在环境中酌情进行必要的审查（例如，技术监督，对策审查[TSCM]，TEMPEST 对策审查）。

T00253	进行粗略二进制分析。
T00254	监督政策标准和实施战略，以确保程序和指南符合网络空间安全政策。
T00255	参与风险治理流程，为其他技术风险提供安全风险，缓解措施和投入。
T00256	评估采购职能在通过采购活动处理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。
T00257	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。
T00258	及时发现，识别和警告可能的攻击/入侵，异常活动和误用活动，并将这些事件与良性活动事件区分开来。
T00259	使用网络防御工具来持续监视和分析系统活动，以识别恶意活动。
T00260	分析确定的恶意活动，以确定利用的弱点，利用方法，对系统和信息的影响。
T00261	协助确定、优先排序和协调关键网络空间防御基础设施和关键资源的保护。
T00262	采用经批准的纵深防御原则和做法（例如，场所多重防御，分层防御，安全稳健性）。
T00263	在系统生命周期的所有阶段确定信息技术（IT）系统特有的安全要求。
T00264	识别在风险评估，审计，检查等期间确定的漏洞，确保行动计划和里程碑或补救计划到位。
T00265	确保成功实施和实现与组织机构的使命和目标一致的安全要求和适当的信息技术（IT）政策和程序的功能。
T00266	根据新的或更新的应用程序执行渗透测试。
T00267	设计针对编程语言弱点和系统和元素中的漏洞的潜在利用的对策和缓解措施。
T00268	定义和记录新系统的实现或系统之间的新接口如何影响当前环境的安全状态。
T00269	设计和开发关键管理功能（与网络空间安全相关）。
T00270	分析用户需求和要求，以规划和执行系统安全开发。
T00271	开发网络空间安全设计以满足特定的操作需求和环境因素（例如访问控制，自动化应用，网络操作，高完整性和可用性要求，多级安全/多级分类处理以及处理敏感分区信息）。
T00272	确保安全设计和网络空间安全开发活动正确记录（提供安全实施的功能描述），并在必要时更新。
T00273	酌情制定和记录关键系统要素的供应链风险。
T00274	创建安全措施的可审计证据。
T00275	支持必要的合规性活动（例如，确保遵循系统安全配置指南，进行合规性监控）。
T00276	根据适当的供应链风险管理实践，参与必要的搜集过程。
T00277	确保所有采办，采购和外包工作满足符合组织机构目标的信息安全要求。
T00278	收集入侵工件（例如，源代码，恶意软件，木马），并使用发现的数据，以减少企业内潜在的网络防御事故。
T00279	担任执法人员的技术专家和联络人，并根据需要解释事件详情。
T00280	根据政策/指南/程序/法规/法律，持续检验组织机构，确保合规。
T00281	预测持续的服务需求，并确保必要的安全假设审查。
T00282	定义和/或实施政策和程序，以确保适当地保护关键基础设施。
T00283	与利益相关者合作，识别和/或开发适当的解决方案技术。
T00284	设计和开发与网络空间安全相关的新工具/技术。
T00285	在数字介质上执行病毒扫描
T00286	执行文件系统取证分析。

T00287	执行静态分析以安装驱动器的“映像”（不必具有原始驱动器）。
T00288	执行静态恶意软件分析。
T00289	部署的取证工具包以在必要时支持操作。
T00290	确定入侵集的策略，技术和过程（TTPs）。
T00291	检查网络拓扑以了解通过网络的数据流。
T00292	推荐计算环境漏洞修正。
T00293	使用元数据（例如，CENTAUR）识别和分析网络流量中的异常。
T00294	在各种所有源数据集（指示和警告）中进行研究，分析和关联。
T00295	针对网络流量使用包分析工具验证入侵检测系统（IDS）警报。
T00296	隔离并删除恶意软件。
T00297	基于网络流量识别网络设备的应用程序和操作系统。
T00298	根据网络流量重建恶意攻击或活动。
T00299	识别网络映射和操作系统（OS）指纹识别活动。
T00300	开发和记录用户体验（UX）要求，包括信息架构和用户界面要求。
T00301	制定和实施网络空间安全独立的审计程序软件/网络/系统，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机构和强制性网络空间安全要求，并在系统管理员和其他网络空间安全人员执行日常工作时准确跟踪。
T00302	制定合同模板，确保满足供应链，系统，网络和运营安全性要求。
T00303	在设计和开发安全应用程序时，确定并利用企业级版本控制系统。
T00304	实现并将系统开发生命周期（SDLC）方法（例如，IBM 统一开发过程）集成到开发环境中。
T00305	对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。
T00306	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。
T00307	分析候选架构，分配安全服务，并选择安全机制。
T00308	分析新出现的趋势的事件数据。
T00309	评估安全控制的有效性。
T00310	协助建立可以在网络空间防御网络工具上实施的签名，以响应 NE 或飞地内的新的或观察到的威胁。
T00311	咨询客户关于软件系统设计和维护。
T00312	与情报分析师协调，关联威胁评估数据。
T00313	设计和记录质量标准。
T00314	开发系统安全上下文，初步系统安全操作概念（CONOPS），并根据适用的网络空间安全要求定义基准系统安全要求。
T00315	开发和提供技术培训，教育他人或满足客户的需求。
T00316	开发或协助基于计算机的培训模块或课程的开发。
T00317	开发或协助课程作业的开发。
T00318	开发或协助开发课程评估。
T00319	制定或协助制定分级和熟练水平标准。
T00320	协助制定个人/集体发展，培训和/或补救计划。
T00321	制定或协助制定学习目的和目标。
T00322	开发或协助开发在职培训材料或计划。

T00323	开发或协助开发测量和评估学习者熟练程度的书面测试。
T00324	直接软件编程和开发文档。
T00325	记录系统的目的和初步系统安全操作概念。
T00326	采用配置管理流程。
T00327	评估网络基础设施漏洞，以增强正在开发的功能。
T00328	评估安全架构和设计，以确定根据收购文件中的要求提议或提供的安全设计和架构的充分性。
T00329	遵循软件和系统工程生命周期标准和过程。
T00330	保持确保的消息传递系统。
T00331	维护事件跟踪和解决方案数据库。
T00332	通知指定的管理人员，网络事故响应人员和网络空间安全服务提供商团队成员疑似网络事件，并根据组织机构的网络事件响应计划阐述事件的历史，状态和进一步行动的潜在影响。
T00333	执行网络防御趋势分析和报告。
T00334	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）。
T00335	构建、安装、配置和测试专用的网络防御硬件。
T00336	撤销，与 T0228 合并
T00337	监督和分配工作给程序员，设计师，技术专家和技术人员和其他工程和科学人员。
T00338	编写详细的功能规范，记录架构开发过程。
T00339	促进组织机构使用知识管理和信息共享。
T00340	作为基础信息技术（IT）操作流程和功能的主要利益相关者，支持服务，提供指导和监控所有重要活动，以便服务成功交付。
T00341	倡导为网络培训资源提供足够的资金，包括内部和行业提供的课程，教师和相关材料。
T00342	分析数据源以提供可操作的建议。
T00343	分析危机情况，以确保公共，个人和资源保护。
T00344	评估所有配置管理（更改配置/发布管理）进程。
T00345	根据教学技术使用的简易性和学生学习，知识转移和满意度来评估教学的有效性和效率。
T00346	评估与调查行为有关的个人受害人，证人或嫌疑人。
T00347	评估源数据的有效性和后续发现。
T00348	协助评估实施和维持专用网络防御基础设施的影响。
T00349	收集指标和趋势数据。
T00350	进行市场分析以识别，评估和推荐商业，GOTS 和开源产品，以便在系统中使用，并确保推荐的产品符合组织机构的评估和验证要求。
T00351	使用统计过程进行假设检验。
T00352	进行学习需求评估和确定需求。
T00353	与系统分析师，工程师，程序员和其他人一起设计应用。
T00354	协调和管理为客户端对端提供的整体服务。
T00355	与内部和外部主题专家协调，以确保现有的资格标准反映组织机构的功能要求，并符合行业标准。

T00356	与组织机构人力利益相关者协调，确保人力资本资产的适当分配和分布。
T00357	创建交互式学习练习，创造有效的学习环境。
T00358	为特权访问用户设计和开发系统管理和管理功能。
T00359	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。
T00360	确定威胁的程度，并建议减轻风险的行动方案或对策。
T00361	开发和促成数据收集方法。
T00362	基于现有的网络工作角色制定和实施标准化的职位描述。
T00363	根据当前的人力资源（HR）政策制定和审查招募、聘用和保留程序。
T00364	制定网络事业领域分类结构，包括建立职业领域入门要求和其他术语，如代码和标识符。
T00365	制定或协助制定网络培训的培训政策和协议。
T00366	从大数据集中开发战略洞察。
T00367	制定网络课程的目标和意图。
T00368	确保网络职业领域根据组织机构的人力资源（HR）政策和指令进行管理。
T00369	确保网络空间劳动力管理政策和流程，符合有关平等机会、多样性和公平雇用/就业的法律和组织机构要求。
T00370	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。
T00371	为软件应用程序，网络或系统设置可接受的限制。
T00372	建立和收集指标，以监控和验证网络空间员工队伍的准备情况，包括分析网络空间员工数据，以评估由合格人员识别，填补和填补的职位的状态。
T00373	建立和监督网络空间职业领域入职和培训资格要求的豁免过程。
T00374	建立网络空间职业道路，以允许职业发展，有意识的发展，以及网络职业领域之间的增长。
T00375	建立人力，人员和资格数据元素标准，以支持网络空间劳动力管理和报告要求。
T00376	根据组织机构要求建立，资源，实施和评估网络空间劳动力管理计划。
T00377	收集客户满意度和内部服务绩效的反馈，以促进持续改进。
T00378	结合风险驱动的系统维护更新流程来解决系统缺陷（周期和周期外）。
T00379	管理与支持服务的信息技术（IT）流程所有者的内部关系，协助操作级别协议（OLA）的定义和协议。
T00380	与教育工作者和培训师一起计划教学策略，如讲座，演示，互动练习，多媒体演示，视频课程，基于网络的课程的最有效的学习环境。
T00381	向技术和非技术受众提供技术信息。
T00382	当前数据的创造性格式。
T00383	自定义算法编程。
T00384	在管理层中酌情提高对网络空间政策和战略的认识，并确保健全的原则被体现在组织机构的使命、愿景和目标中。
T00385	基于数据分析和发现，向关键利益相关者提供可行的建议。
T00386	在司法过程中向审判律师提供刑事调查支持。
T00387	审查和应用网络空间职业领域资格标准。
T00388	审查和应用与网络空间劳动力相关或对网络劳动力有影响的组织机构政策。
T00389	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，确保所有未决问题得到跟踪。

T00390	审查/评估网络空间工作人员的有效性，以调整技能和/或资格标准。
T00391	支持将合格的网络空间劳动力人员纳入信息系统生命周期开发过程。
T00392	利用技术文档或资源来实现新的数学，数据科学或计算机科学方法。
T00393	验证可测试性的规范和要求。
T00394	与其他服务管理者和产品所有者合作，平衡和优先处理服务，以满足客户的整体需求，约束和目标。
T00395	在行动审核后撰写和发布。
T00396	根据分析师的目标使用适当的工具处理图像。
T00397	执行 Windows 注册表分析。
T00398	在通过动态分析识别入侵之后，对运行的系统执行文件和注册表监视。
T00399	将介质信息输入已获取的数字介质的跟踪数据库（例如，产品跟踪工具）。
T00400	关联事件数据和执行网络空间防御报告。
T00401	维护可部署的网络空间防御工具包（例如专门的网络空间防御软件/硬件），以支持 IRT 任务。
T00402	在数据管理系统的设计中有效分配存储容量。
T00403	在 Windows 和 UNIX 系统（例如，执行以下任务：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）中读取，解释，写入，修改和执行简单脚本（例如 PERL，VBS） 。
T00404	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。
T00405	利用开放源语言如 R 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检验，普通最小二乘回归，一般线）。
T00406	确保设计和开发活动正确记录（提供实施的功能描述），并在必要时更新。
T00407	必要时参与采购过程。
T00408	解释和应用适用的法律，法规和监管文件，并纳入政策。
T00409	在产品设计，开发和启动前阶段对原型设计和过程问题进行故障排除。
T00410	识别安全相关功能，以找到新功能开发的机会，以利用或减轻漏洞。
T00411	识别和/或开发逆向工程工具以增强功能和检测漏洞。
T00412	进行采购系统和软件的进出口审查。
T00413	开发数据管理功能（例如，基于云的集中式密码密钥管理），以包括对移动工作人员的支持。
T00414	制定供应链、系统、网络、性能和网络空间安全要求。
T00415	确保供应链，系统，网络，性能和网络空间安全要求包含在合同模板中并交付。
T00416	通过利用现有的公钥基础设施（PKI）库并在适当时引入证书管理和加密功能来启用具有公钥的应用程序。
T00417	适当时，在设计和开发安全应用程序（例如，企业 PKI，联合身份服务器，企业防病毒解决方案）中，确定并利用企业范围的安全服务。
T00418	安装、更新系统/服务器并对其进行故障排除。
T00419	获得并保持有关宪法问题的相关法律、法规、政策、协议、标准、程序或其他发布的工作知识。
T00420	管理测试平台，测试和评估应用程序，硬件基础设施，规则/签名，访问控制以及由服务提供商管理的平台配置。
T00421	管理组织机构的显性知识产权的索引/编目，存储和访问（例如，硬拷贝文件，

	数字文件）。
T00422	实施数据管理标准，要求和规范。
T00423	分析计算机生成的威胁用于反情报或犯罪活动。
T00424	分析并向利益相关者提供信息，以支持开发安全应用或修改现有安全应用。
T00425	分析组织机构网络空间政策。
T00426	分析软件，硬件或互操作性测试的结果。
T00427	分析用户需求和要求以规划架构。
T00428	分析安全需求和软件需求，以确定在时间和成本限制和安全任务中的设计可行性。
T00429	评估政策需求，并与利益相关者合作制定管理网络活动的政策。
T00430	收集和保存用于起诉计算机犯罪的证据。
T00431	检查系统硬件可用性，功能，完整性和效率。
T00432	收集和分析入侵工件（例如，源代码，恶意软件和系统配置），并使用发现的数据来减少企业内潜在的网络防御事故。
T00433	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的最佳方法。
T00434	执行诉状的框架，以正确识别涉嫌违反法律，法规或政策/指导的行为。
T00435	执行定期系统维护，包括物理和电子清洁，磁盘检查，常规重新启动，数据转储和测试。
T00436	进行程序和软件应用程序的试运行，以确保生成所需的信息，说明和安全级别正确。
T00437	将培训和学习与业务或任务要求相关联。
T00438	在专门的网络空间防御系统（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。
T00439	检测和分析加密数据，隐写，备用数据流和其他形式的隐藏数据。
T00440	捕获和集成在灾难性故障事件后部分或全部系统恢复所需的基本系统功能或业务功能。
T00441	定义和集成当前和未来的任务环境。
T00442	创建针对观众和物理环境的培训课程。
T00443	提供针对观众和物理/虚拟环境的培训课程。
T00444	将概念、程序、软件、设备和/或技术应用程序提供给学生。
T00445	设计/整合网络空间战略，概述与组织机构战略计划相一致的愿景、使命和目标。
T00446	设计、开发、集成和更新提供机密性、完整性、可用性、身份验证和不可抵赖性的系统安全措施。
T00447	设计硬件、操作系统和软件应用程序，以充分满足需求。
T00448	开发满足用户需求所需的企业架构或系统组件。
T00449	设计以确保满足所有系统和/或应用程序的安全要求。
T00450	根据需求设计培训课程和课程内容。
T00451	参与培训课程和课程内容的开发。
T00452	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机构智力资本的访问。
T00453	确定和开发潜在客户并确定信息来源，以识别和/或起诉入侵或其他犯罪的责任方。

T00454	根据适用的准则定义基线安全要求。
T00455	开发软件系统测试和验证程序，编程和文档。
T00456	开发安全软件测试和验证程序。
T00457	开发系统测试和验证程序，编程和文档。
T00458	遵守组织机构的系统管理标准操作程序。
T00459	实施数据挖掘和数据库应用程序。
T00460	开发和实施数据挖掘和数据仓库计划。
T00461	实施和执行本地网络使用政策和程序。
T00462	根据系统可用性要求，开发程序和测试故障，转移系统操作到备用站点。
T00463	开发新系统或修改系统的成本估算。
T00464	为组件和接口规范开发详细的设计文档，以支持系统设计和开发。
T00465	制定实施准则。
T00466	制定缓解策略以解决成本，进度，绩效和安全风险。
T00467	确保培训达到网络空间安全培训，教育或意识的目标和目的。
T00468	诊断和解决客户报告的系统事故，问题和事件。
T00469	分析和报告组织机构的安全状况趋势。
T00470	分析和报告系统安全状态趋势。
T00471	记录数字和/或相关证据的原始条件（例如，通过数字照片，书面报告，散列函数检查）。
T00472	起草，配备和发布网络空间政策。
T00473	根据需要记录和更新所有定义和架构活动。
T00474	向检查长，隐私官，监督和合规人员提供有关遵守网络空间安全政策和相关法律法规要求的法律分析和决策。
T00475	基于最小特权和需要知道的原则评估适当的访问控制。
T00476	评估法律、法规、政策、标准和程序变更的影响。
T00477	确保灾难恢复的执行和操作的连续性。
T00478	向管理层、员工或客户提供有关法律、法规、政策、标准或程序的指导。
T00479	使用信息技术（IT）系统和数字存储介质来解决，调查和/或起诉针对人员和财产的网络犯罪和欺诈。
T00480	识别组件或元素，分配全面的功能组件以包括安全功能，并描述元素之间的关系。
T00481	确定和解决网络空间人力规划和管理问题（例如招聘，录用和培训）。
T00482	根据趋势分析提出建议，以增强软件和硬件解决方案，以提高客户体验。
T00483	通过实施任何网络空间防御工具（如工具和签名测试和优化）确定潜在冲突。
T00484	记录信息系统和网络以及文档的保护需求（即安全控制）。
T00485	实施安全措施以根据需要解决漏洞，降低风险并向系统或系统组件推荐安全更改。
T00486	在企业内部实施针对专用网络防御系统的风险管理框架（RMF）/安全评估和授权（SA&A）要求，并为其记录和维护记录。
T00487	促进实施新的或修订的法律，法规，行政命令，政策，标准或程序。
T00488	实现新系统或现有系统的设计。
T00489	根据既定程序实施系统安全措施，以确保机密性，完整性，可用性，认证和不可否认性。

T00490	安装和配置数据库管理系统和软件。
T00491	根据组织机构的标准为系统用户安装和配置硬件，软件和外围设备。
T00492	确保跨域解决方案（CDS）在安全环境中的集成和实施。
T00493	领导和监督预算、人员配置和合同。
T00494	管理帐户、网络权限以及访问系统和设备。
T00495	管理认证包（例如，ISO / IEC 15026-2）。
T00496	执行信息技术（IT）资源的资产管理/清点。
T00497	管理信息技术（IT）规划流程，以确保开发的解决方案满足客户要求。
T00498	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。
T00499	减轻/纠正在安全/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。
T00500	修改和维护现有软件以纠正错误，使其适应新硬件，或升级接口并提高性能。
T0501	监控和维护系统/服务器配置
T0502	监控和汇报客户端计算机系统性能
T0503	监控外部数据源（比如网络空间防御厂商网站、计算机应急响应团队、安全焦点）保持对网络空间防御威胁情况的情况，并且确定那些可能对企业产生影响的安全问题。
T0504	评估和监控与系统实现和测试相关的网络空间安全主题。
T0505	在规划和管理服务中，严格监控网络空间政策、原则和实践的执行应用情况。
T0506	与利益相关者讨论，对提议的政策变化情况寻求一致。
T0507	对系统组件的安装、实现、配置和支持提供监管。
T0508	对所有应用检查，确保最小安全需求原则正确应用。
T0509	进行信息安全风险评估
T0510	协调事件响应功能
T0511	对正在开发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	进行可操作性测试
T0514	对故障系统/服务器硬件进行诊断
T0515	对故障系统/服务器硬件进行修复。
T0516	进行安全程序测试、审查和/或评估，识别代码中潜在的缺陷，减轻漏洞危害。
T0517	集成关于安全架构差距识别的结果。
T0518	进行安全审查，识别架构中的安全漏洞。
T0519	对课堂教学技术和形式（比如演讲、演示、交互式练习、多媒体演示）进行规划和协调，创造最高效的学习环境
T0520	对非课堂教学的教育技术和形式进行规划（比如视频课程、指导和网络课程）
T0521	规划实现策略，确保企业组件可以集成到一起并（与企业目标）对齐。
T0522	准备法律和其他相关文档（比如证词、简短声明、宣誓书、公告、上诉、答辩、证据显示）
T0523	根据法律标准和要求，准备编写调查报告。
T0524	通过组织机构的操作流程和系统，促进信息所有者/用户之间的信息共享。
T0525	提供企业网络空间安全和供应链风险管理指南
T0526	对于重大威胁和漏洞，提供网络空间安全建议，确保领先。
T0527	对实现计划和标准操作流程中信息系统安全相关部分，提供输入内容

T0528	为实现计划、标准操作流程、维护文档和维护培训材料提供输入内容
T0529	为网络空间管理、人员和用户提供政策指南
T0530	编写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	为恢复潜在相关信息，对取证图像和其他数据源（比如易失数据）进行审查。
T0533	审查、进行或参与网络空间程序和项目的审计
T0534	对课程内容的准确性、完整性检查和当前情况（比如课程内容文档、课程计划、学生用书、考试、课程表、课程描述）进行定期审查/修订
T0535	基于之前培训课程的反馈，对课程内容给出修订建议。
T0536	在个人专业领域内承担内部顾问和专家的角色（比如技术、版权、平面媒体、电子媒体）
T0537	协助 CIO 指定网络空间相关的政策
T0538	支持测试和评估活动
T0539	对软硬件进行测试、评估和验证，确定与已定义规格和要求的合规性。
T0540	记录和管理测试数据
T0541	跟踪系统需求、设计（系统）组件，进行差距分析。
T0542	将建议的能力（需求）转换为技术需求
T0543	使用数据雕刻技术（比如 FTK-Foremost）提取数据进行进一步分析
T0544	验证系统架构的稳定性、互操作性、可移植性和/或可扩展性。
T0545	与利益相关者工作解决计算机安全事件和漏洞合规性问题。
T0546	编写发布网络空间防御建议、报告，向特定用户编写针对事件调查的白皮书。
T0547	研究评估可用的技术和标准，满足客户需求。
T0548	为灾难恢复、操作计划意外处理和（业务）持续，提供建议和输入（资料）。
T0549	针对相关技术关注领域（比如本地计算环境、网络和基础设施、飞地边界、支撑设施和应用），进行技术（技术评估）和非技术（人员或操作评估）风险和漏洞评估，
T0550	给出建议，选择高性价比安全控制方案，降低风险（比如信息保护、系统和流程）
T0551	起草、发布供应链安全和风险管理文档
T0552	审查、批准供应链安全/风险管理政策
T0553	应用网络空间安全的功能（比如加密、访问控制、身份管理）降低漏洞（利用）机会。
T0554	确定并记录软件补丁或已经发布的、可能使软件免受漏洞影响的扩展版本
T0555	记录多个系统之间，一个新系统或新接口的不同实现，对当前和目标环境的影响，包括但不限于对于安全态势的影响。
T0556	评估、设计网络空间相关的安全管理功能
T0557	集成网络空间相关的关键管理功能
T0558	分析用户需求，规划和进行系统开发
T0559	设计满足特定业务和环境需求（比如访问控制、自动化应用、网络操作）
T0560	协作进行网络空间安全设计，满足特定业务和环境需求（比如访问控制、自动化应用、网络操作、高完整性和可用性需求、多级分类的多层次安全/处理，处理敏感信息隔离 SCIF）
T0561	准确的目标描述

T0562	调整收集操作或计划，解决发现的问题/挑战，并且与整体的操作需求收集同步。
T0563	为分析、设计、开发和满足目标要求的能力获取，提供输入项。
T0564	分析反馈意见，确定满足需求的（信息）收集产品和服务的范围。
T0565	分析收到的搜集请求
T0566	分析自身的业务架构、工具和程序，寻找提高性能的方法。
T0567	分析目标业务架构，寻找获得访问（权限）的方法
T0568	分析计划、指令、指南和可能影响收集管理业务结构和需求（比如持续时间、范围、通信需求、跨部门/国际协议）的政策因素。
T0569	回复信息咨询
T0570	利用已经被授权的网络空间能力，来访问目标网络
T0571	应用政策和流程专业知识，促进开发、谈判、内部人力计划和/或备忘录协议（签订）
T0572	进行网络空间收集、环境准备和具备职业能力，让新的利用和/或持续的收集操作或可支持客户需求的东西（可以运作）
T0573	评估、应用操作环境因素，和收集管理过程风险分析
T0574	应用、遵守适用的法规、法律、规定和政策
T0575	对操作计划活动，协调情报支持
T0576	评估所有来源情报，支持网络空间操作目标，提供推荐目标。
T0577	评估现有信息交换和管理系统的效率
T0578	根据规定规格，对信息收集资产进行效率评估
T0579	评估目标漏洞和/或业务操作能力，确定行动过程
T0580	使用可用的能力和方法，评估收集效率，满足信息差距优先级，相应的调整搜集策略和搜集需求。
T0581	建议和协助跨机构合作伙伴，确定发展最佳实践，促进业务支持实现组织机构目标。
T0582	为行动发展提供专业知识
T0583	为一个共同的业务构想，提供相关专业知识
T0584	维护一个共同的情报构想
T0585	为网络空间特定的操作指标，提供相关专业知识
T0586	帮助协调、验证、管理全源搜集需求、计划和/或行动
T0587	帮助信息需求优先级的指定和完善
T0588	为措施的有效性和性能改善，提供专业知识
T0589	帮助识别情报收集的不足。
T0590	需要时，情报支持计划可以跨合作伙伴进行同步。
T0591	对目标基础设施利用行动进行分析
T0592	为网络空间相关成功标准的鉴别，提供输入项。
T0593	做威胁和/或目标当前情况的简报
T0594	建立和维护电子目标文件夹
T0595	按照分类指南对文档进行分类
T0596	信息满足后的类似需求
T0597	与相关领域的情报分析师/目标机构合作
T0598	与开发机构合作，创建、部署达到目标所需的工具。
T0599	与其他客户、和网络空间相关领域的情报和目标机构合作

T0600	在目标访问和操作问题上，与内部和外部的合作伙伴机构合作
T0601	与其他团队成员和合作机构合作，开发多样的信息材料程序（比如网页、简报、打印材料）
T0602	与客户合作，定义信息需求
T0603	沟通新的进展、突破、挑战和关于领导力的经验教训，以及内部和外部客户（的情况）。
T0604	将所分配资产和可用资产与需求分析得到的收集要求进行比较
T0605	对在组织结构搜集目标的搜集管理活动中获得的经验教训进行汇总
T0606	对情报的所有来源数据或特定目标的漏洞价值数据进行汇总、集成和/或解释。
T0607	确定、进行目标的通信分析，识别支持业务所需的关键信息
T0608	对物理和逻辑数字技术（比如无线、SCADA、电信技术）进行分析，寻找潜在的访问路径。
T0609	对无线计算机和数字网络进行访问授权
T0610	对无线计算机和数字网络进行（信息）收集和处理
T0611	进行业务终止评估
T0612	对无线计算机和数字网络进行利用
T0613	按照既定准则和程序，对收集要求进行正式的、非正式的协调。
T0614	进行独立的、深入的目标和技术分析，包括导致访问（入侵）的特定目标信息（比如文化的、组织的、政治的）在内。
T0615	进行深入研究分析
T0616	对网络中的系统进行网络探测和漏洞分析
T0617	进行节点分析
T0618	从已经部署的系统中，进行线上行动来控制和数据泄露。
T0619	从已经部署的、自动化系统中，进行线上的、线下的行动来控制和数据泄露。
T0620	通过各种在线工具进行开源数据收集。
T0621	进行质量控制，来确定网络信息收集的有效性和相关性。
T0622	制定、审查和实施各级规划指导，支持网络空间行动。
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	在应用优先信息需求时，考虑收集资产和资源的效率和有效性。
T0626	使用既定指南和程序，构建收集计划和矩阵
T0627	对网络空间业务的关键行动贡献力量
T0628	必要时，对组织机构的决策支持工具开发贡献力量
T0629	对网络空间运营政策、绩效标准、计划、和与内外部决策者批准的方案，进行实施、人员配置和协调。
T0630	将情报纳入网络空间运营计划的整体设计中。
T0631	协调分配搜集资产，让优先处理的搜集需求符合搜集标准要求。
T0632	在合适文档中对收集计划的内容进行协调
T0633	与合适的合作伙伴一起，协调进行目标审查。
T0634	对收集资产和资源重新进行任务分配和方向选择
T0635	协调情报和网络防御伙伴，获得相关关键信息
T0636	与情报规划人员协调，确保收集管理者可以收到信息需求。
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、创造和跟踪情报需求
T0639	协调、同步、起草网络空间运营计划中情报（相关）的部分
T0640	使用情报评估，对付目标可能的行动。
T0641	创造周全的利用策略，确定利用技术或可使用漏洞。
T0642	持续关注内外部网络空间机构的结构、优势、人员和技术
T0643	向目标部署工具，并且在部署后利用他们（比如后面、探测）
T0644	监测目标网络和主机相关漏洞，并做出相应响应。
T0645	确定解决目标、指南和操作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	确定那些影响任务、收集、处理、利用和传播架构形式和功能的因素。
T0648	确定最适合特定网络空间操作目标的指标（比如有效性指标）
T0649	确定所有具有访问收集资产权限的组织机构和层次
T0650	确定给定目标在使用什么技术
T0651	开发一种方法，将收集的报告和突出的需求进行比较，发现信息差距。
T0652	开发目标资料相关的所有来源情报
T0653	利用分析技术，获得更多目标信息
T0654	制定、维护周全的和/或紧急的计划
T0655	制定、审查具体的网络行动计划，将其纳入更广泛的规划活动中。
T0656	制定、审查情报指南，将其纳入对网络行动规划执行的支撑中。
T0657	收集操作每一个阶段的要求，制定协调指南
T0658	开发网络空间运营计划和指南，确保执行和资源分配决策与组织机构目标一致。
T0659	对网络行动要求，提供详细的情报支持。
T0660	开发用来回答优先信息要求的信息需求
T0661	制定有效性指标和性能指标
T0662	根据领导指导、优先安排和/或业务重点分配（信息）收集资产
T0663	制定效率评估和操作评估的必需材料
T0664	开发新技术，来获得和保持对目标系统的访问能力。
T0665	制定或参与标准制定，从外部伙伴那里提供、请求和/或得到支持，同步网络空间操作。
T0666	指定、形成国际网络空间参与战略、政策和行动，满足组织机构目标。
T0667	制定可能的行动方针
T0668	开发向搜集管理者、资产管理者和处理、利用、传播中心提供反馈的程序。
T0669	为合作伙伴规划、业务和能力方针制定战略和流程
T0670	对适当的计划过程和政策进行制定、实施和变更建议。
T0671	制定、维护、评估与外部伙伴制定的网络空间合作安全协议。
T0672	制定、记录、验证网络空间操作战略和规划文档
T0673	向决策者汇报收集的问题
T0674	传达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	起草网络空间情报收集和产品需求
T0677	在 Windows 和 Unix 系统中编辑或执行简单脚本（比如 Perl、VBS）
T0678	让客户了解他们的情报需求。
T0679	确保业务计划有效的切入到当前业务中

T0680	确保情报规划行动纳入业务规划时间表，并与之同步。
T0681	建立可替代处理、利用和传播路径，解决已确定的问题
T0682	验证收集要求和关键信息需求直接的联系，以及验证领导优先情报需求
T0683	使用已经批准的指南和/或流程，建立处理、利用和传播的管理活动。
T0684	评估网络空间行动产生的操作效果
T0685	评估威胁决策过程
T0686	识别威胁漏洞
T0687	识别蓝牙漏洞威胁
T0688	评估预期效果的可用能力，推荐有效的解决方案
T0689	评估收集的信息和/或产生的情报对信息需求的满足程度
T0690	评估情报支持规则周期
T0691	评估影响现有网络情报能力就业情况的条件
T0692	生成、评估网络分析策略的有效性
T0693	评估收集操作与操作要求之间同步的程度
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，了解目标的意义
T0696	使用各种方法或工具，渗透利用网络设备、安全设备和/或终端设备或环境。
T0697	通过物理的或无线的方式，促进（获得）访问（权限）
T0698	促进不断更新的情报、监视和可视化输入到常见的操作图景管理者。
T0699	促进内部外部决策者之间的沟通，同步和整合支撑（企业）目标的行动方针。
T0700	促进在整个网络空间操作社区分享“最佳实践”和“经验教训”。
T0701	与开发人员合作，传递工具需求提交的目标和技术知识，加强工具开发
T0702	基于现有情报学科能力的知识，制定收集策略。收集与多学科收集能力和入口与目标和他们观测相一致的方法。
T0703	收集和分析数据（比如有效性措施）确定有效性，并提供后续活动的报告。
T0704	将网络空间操作和通信安全支持计划，纳入组织机构目标
T0705	结合情报获取和反情报窃取（情况）支持计划制定
T0706	通过传统技术或其他替代技术收集网络信息（比如社交网络分析、调用链、流量分析）
T0707	生成信息需求
T0708	识别威胁的手段和方法
T0709	确定所有可用的合作伙伴的情报能力和局限，支持网络空间操作
T0710	识别、评估威胁的关键能力、要求和漏洞
T0711	确定、起草、评估和确定相关情报或信息需求的优先级
T0712	和外部合作伙伴一起确定和管理安全合作的优先事项
T0713	确定、提交情报需求，以便指定信息需求优先事项
T0714	确定作为与指定机构和职能组进行协调机制的协作论坛。在这个机制中可以协调流程、职能和产生情况。
T0715	确定收集的差距，和针对目标潜在的收集策略。
T0716	与指定的收集部门确定协调需求和程序。
T0717	识别关键目标元素
T0718	识别情报的差距和不足
T0719	识别网络空间情报差距和不足

T0720	识别我们对目标技术的理解差距，创造新的收集方法
T0721	识别可能破坏和/或降低处理、利用和传播架构效果的问题
T0722	识别网络组件和他们的功能，以便实现分析和目标开发
T0723	确定针对优先信息需求应用可能的收集要求
T0724	确定网络中潜在的优势和弱点
T0725	识别、降低收集管理能力的风险，支持规划、操作和目标周期
T0726	确定适用情报环境准备衍生产品的需求、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	根据威胁因素提供制定行动方针的输入项
T0729	将新发布的或修订的网络空间运营伙伴行动政策和指南的潜在影响，向外部合作伙伴通告。
T0730	使用既定流程向利益相关者（比如搜集管理者、资产管理管理者、处理、利用和传播中心）通报评估结果
T0731	发起任务指导请求，协助收集管理
T0732	与其他机构整合网络空间规划/目标工作
T0733	对环境准备评估进行解释，确定行动方针
T0734	发布信息需求
T0735	领导和协调对操作规划情报的支持
T0736	领导或启动利用操作，支持组织机构的目标和靶标需求。
T0737	将重点采集需求和最佳资产和资源联系起来
T0738	关注硬件和软件技术进步（比如参加培训或会议、阅读）以及他们的潜在影响
T0739	与参与网络规划或相关领域的内外部伙伴保持联系
T0740	保持有机操作基础设施的态势感知和功能
T0741	保持网络空间相关情报和任务的态势感知能力
T0742	保持合作伙伴能力和行动的情况掌握
T0743	保持态势感知，操作环境变化时，确定是否需要对计划进行审查
T0744	维护靶标列表（比如 RTL, JTL, CTL 等）
T0745	提出建议，指导收集，支持客户需求
T0746	必要时修改搜集需求
T0747	监控、评估网络空间整体操作，寻找满足组织机构目标的机会
T0748	对威胁处置、行动、策略、能力、目标等网络空间操作告警问题集相关的变化，进行监控和汇报。
T0749	对以验证的威胁行动进行监控和汇报
T0750	监控重新分配的收集工作的完成情况
T0751	包含对组织机构或合作伙伴利益充满恶意内容的开源网站进行监控。
T0752	监控操作环境，汇报那些符合领导优先信息要求的对抗活动
T0753	监控处理、利用和传播架构的状态和有效性
T0754	监控目标网络，提供目标通信变化或处理故障的指示和警告
T0755	监控操作环境，关注收集操作管理过程中的潜在因素和风险。
T0756	操作和维护自动化系统，获取并维持对目标系统的访问
T0757	优化收集资产和资源的组合，提高优先情报需求相关的关键信息的有效性和效率。
T0758	生成及时的、融合的、所有来源的网络空间操作情报和/或指示和告警情报产品。

	（比如威胁评估、简报、情报研究、国家研究）
T0759	协助审查和完善政策，包括赞同或不赞同这些政策的结果评估。
T0760	需要时，向规划组、协调组、任务组提供专业知识
T0761	需要时，提供主题专家，支持规划/发展论坛和工作组。
T0762	在行动过程中提供主题专家
T0763	与网络空间行动中的内外部合作伙伴，形成长期的战略规划工作。
T0764	提供主题专家，与内外部的网络操作伙伴进行规划工作
T0765	提供主题专家，发展练习
T0766	提出与外部协调小组互动管理的政策
T0767	进行内容和/或元数据分析，满足组织机构目标
T0768	进行网络空间行动，降低/删除驻留在计算机和计算机网络中的信息。
T0769	进行自动目标锁定行动
T0770	寻找网站特征
T0771	提供主题专家，寻找网站特征
T0772	为（项目）练习，准备和提供主题专家
T0773	基于平台的能力，制定各平台的搜集需求优先顺序
T0774	进行泄露数据分析和/或向客户传达。
T0775	进行网络重建
T0776	形成目标系统分析产品
T0777	对网络或系统管理员和他们的行动进行配置、描述
T0778	对目标和他们的行动进行配置、描述
T0779	为操作和情报决策者提供建议/帮助，重新分配收集资产和资源，应对操作情况的动态变化。
T0780	提供咨询和宣传支持，帮助收集计划成为战略计划和其他适用计划的一部分。
T0781	提供目标点和再接入建议
T0782	为有效性评估提供分析和支持
T0783	为核心的内外部利益相关方适时提供情报支持
T0784	为情报支持计划的输入项，提供网络空间关注的指南和建议
T0785	提供必要的评估和反馈，提高情报生产、情报汇报、搜集需求和运作的质量。
T0786	为领导和客户提供信息和评估，开发细化目标、支持操作的计划和执行，评估操作影响。
T0787	为网络空间操作目标、优先级、策略、规划和程序的发展和完善，提供输入。
T0788	为行动后的效果评估提供输入和协助
T0789	为规划和指南的制定提供输入和协助
T0790	为领导接受，提供目标有效性评估指标
T0791	为业务支持计划，提供行政和后勤投入
T0792	为指定的演习、计划行动和时效性操作提供情报分析和支持
T0793	为指定的演习和/或时效性操作提高有效支持
T0794	提供操作和再接入建议
T0795	提供内外部伙伴之间的规划支持
T0796	提供实时的、可行动的地理位置信息
T0797	提供符合领导目标的靶标建议
T0798	提供靶标产品和指定的靶标支持

T0799	提供时效性靶标支持
T0800	对可能影响组织机构目标、资源或能力，紧迫或恶意的企图和行动，提供及时的通告
T0801	酌情的建议用于细化，适应，终止和执行业务计划。
T0802	审查适当的信息来源，以确定收集的信息的有效性和相关性
T0803	以图表或报告格式重建网络。
T0804	旨在实现网络效应的行动期间，针对目标记录信息收集和/或环境准备活动。
T0805	报告情报导致的重大网络事件和入侵。
T0806	按照批准的指导和/或程序，使用纪律的资产和资源集合，请求专门规程加工、开发、收集和传播信息
T0807	在开放和分类来源的新兴技术（计算机和电话网络，卫星，有线和无线）的研究通信趋势。
T0808	审查和了解组织机构的领导目标和规划指导。
T0809	审查分配收集资产的能力。
T0810	审查情报收集指导的准确性/适用性。
T0811	优先收集要求和基本信息的审查清单。
T0812	根据需要查看和更新总体收集计划。
T0813	审查，批准，确定优先级并提交研究，开发和/或获取网络功能的操作要求。
T0814	根据最佳资产和资源的可用性修改收集矩阵。
T0815	审查和最小化信息以保护来源和方法。
T0816	适用网络情报规划工作。
T0817	通过识别可以协助调查复杂或异常情况的主题专家，作为合作伙伴团队的信息渠道。
T0818	担任与外部合作伙伴的联络人。
T0819	征求和管理要求人员对收集要求的质量，及时性和有效性的完整反馈。
T0820	指定收集计划和/或操作环境的变更，这些需要重新安排或重新指导收集资产和资源。
T0821	指定在短期内必须执行的特定于纪律的集合和/或任务。
T0822	向搜集需求管理部门提交信息请求，加工成为搜集请求。
T0823	提交或回应网络营销解除请求
T0824	支持识别和记录附带效应。
T0825	同步网络国际参与活动和相关资源需求。
T0826	同步网络部分的安全合作计划。
T0827	使用可用的协作功能和技术来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工具进行操作使用。
T0829	针对目标工具测试内部开发的工具和技术。
T0830	使用既定程序跟踪信息请求的状态，包括处理为收集请求和生产要求的状态。
T0831	将收集请求转换为适用的特定专业收集要求。
T0832	使用反馈结果（例如，获得的经验教训）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、情报分析员和搜集管理者紧密合作，确保情报需求和收集计划准

	确和及时。
T0835	与计划者、分析师和搜集管理者密切合作，确定情报差距，确保情报需求准确和及时。
T0836	记录传达事件和/或练习结果的经验教训。
T0837	影响组织机构目标的语言和文化问题向管理者和运营商提供咨询。
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，以便于分析，定位和收集机会。
T0840	在内部和/或外部组织机构方面进行协作，以加强收集，分析和传播。
T0841	进行全源目标研究，包括以目标语言使用开源资源。
T0842	对目标通信进行分析，以确定支持组织机构目标的基本信息。
T0843	进行质量审查，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，分析和处理。
T0845	识别网络威胁的策略和方法。
T0846	识别全球网络内的目标通信。
T0847	保持对目标通信工具，技术和目标通信网络（例如，容量，功能，路径，关键节点）的特征的认识及其对目标，收集和分析的潜在影响。
T0848	向搜集管理者提供反馈，以加强未来收集和分析。
T0849	在初始来源数据中执行外语和方言识别。
T0850	执行或支持技术网络分析和映射。
T0851	提供要求和反馈，优化语言处理工具的开发。
T0852	适当的执行社交网络分析和文件
T0853	扫描，识别和确定目标图形（包括机器对机器通信）和/或语音材料的优先级。
T0854	向适当的客户提供关键或时间敏感的信息。
T0855	以目标语言转录目标语音资料。
T0856	翻译（例如逐字，主旨和/或摘要）目标图形资料。
T0857	翻译（例如，逐字，主旨和/或摘要）将目标语音资料。
T0858	在计算机程序中识别外语术语（例如，注释，变量名称）。
T0859	提供近实时语言分析支持（例如实时操作）。
T0860	以目标语言识别与网络/技术相关的术语。
T0861	与总顾问，外部事务和业务合作，确保现有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，关键部门和委员会合作，确保组织机构拥有并保持适当的隐私和保密同意，授权表格和反映当前组织机构和法律实践和要求的信息通知和材料。
T0863	与适当的管理机构协调一致，确保涉及公民权利，公民自由和隐私考虑的方案，政策和程序得到综合和全面的处理。
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	保持现有的适用联邦和州隐私法律和认证标准的知识，并监督信息隐私技术的进步，以确保组织机构的适应性和合规性
T0867	确保所有处理和/或数据库在必要时向本地隐私/数据保护机构注册。
T0868	与业务团队和高级管理层合作，确保对隐私和数据安全问题的“最佳做法”的认识。

T0869	与组织机构高级管理层合作建立一个组织范围的隐私监督委员会
T0870	担任隐私监督委员会活动的领导角色
T0871	协调网络隐私和安全政策和程序
T0872	与网络空间安全人员就安全风险评估过程进行协作，以解决隐私合规性和风险缓解
T0873	与高级管理层联系制定收集，使用和共享信息的战略计划，以最大限度地发挥其价值，同时遵守适用的隐私条例
T0874	为公司人员提供有关信息资源和技术的战略指导
T0875	协助安全主任开发和实施信息基础设施
T0876	与公司合规官协调一下：记录和报告任何隐私违规证据的自我披露程序。
T0877	与适用的组织单位合作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人
T0879	担任信息系统部门的联络人
T0880	开发隐私培训材料和其他沟通，增加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，直接，交付或确保向所有员工，志愿者，承包商，联盟，业务伙伴和其他适当的第三方提供初始隐私培训和指导
T0882	进行持续的隐私培训和意识活动
T0883	与外部事务合作，与隐私和数据安全问题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	与组织机构行政，法律顾问和其他有关方面合作，代表组织机构的信息隐私权利与外部各方，包括政府机构，承诺采取或修改隐私立法，法规或标准。
T0885	定期向董事会，CEO 或其他负责任个人或委员会报告隐私计划的状况
T0886	与外部事务合作，回应有关消费者和员工数据的新闻和其他查询
T0887	为组织机构的隐私计划提供领导权
T0888	直接和监督隐私专家，并与全球高级管理人员协调隐私和数据安全计划，以确保整个组织机构的一致性
T0889	确保对不遵守组织机构内的劳动力个人所有的隐私政策的隐私惯例和制裁一致的应用程序的合规性，扩大劳动力和人力资源的合作以及所有业务伙伴的信息安全官，行政和法律顾问均适用
T0890	对不遵守企业隐私政策和程序制定适当的制裁措施
T0891	解决关于不遵守公司隐私政策或信息实务通知的指控
T0892	制定和协调隐私的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，并确保其符合企业隐私和数据安全目标和政策。
T0894	制定和管理企业范围的程序，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	建立过程，用于接收，记录，跟踪，调查和采取行动，对所有有关组织机构的隐私政策和程序的投诉
T0896	建立管理和业务机制，追踪获得受保护的健康信息的机会，并在组织机构的范围内并按照法律要求，允许合格的个人审查或收到有关此类活动的报告
T0897	领导规划，设计和评估隐私和安全相关的项目
T0898	建立内部隐私审计计划

T0899	根据法律，监管或公司政策的变化，定期修改隐私计划
T0900	提供开发指导，协助组织机构管理和行政管理与法律顾问协调组织机构的信息隐私政策和程序的识别，实施和维护。
T0901	确保对使用，收集和披露个人信息的技术的使用保持并且不会侵蚀隐私保护
T0902	监控系统开发和操作的安全性和隐私遵守
T0903	对个人信息私隐的建议规则进行隐私影响评估，包括收集的个人信息类型和受影响人数
T0904	与组织机构的其他合规和业务评估职能协调，定期进行信息隐私影响评估和持续合规监测活动
T0905	检查所有与系统相关的信息安全计划，以确保安全和隐私惯例之间的一致性
T0906	与涉及发布受保护信息任何方面的所有组织机构人员合作，确保与组织机构的政策，程序和法律要求相协调
T0907	负责个人信息和/或保护信息发布或披露的个人要求
T0908	制定和管理审批供应商遵守隐私和数据安全政策和法律要求的程序
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，以确保所有隐私问题，要求和责任得到解决
T0910	作为或与合作伙伴合约的律师合作
T0911	减轻员工或业务伙伴使用或披露个人信息的影响
T0912	制定和应用纠正措施程序
T0913	对与组织机构的隐私政策和程序有关的所有投诉采取行动，与其他类似职能协调配合，并在必要时向其提供法律顾问
T0914	支持组织机构的隐私合规计划，与隐私官，首席信息安全官员和其他业务领导密切合作，确保遵守联邦和州的隐私法律法规
T0915	确定和纠正潜在的公司合规差距和/或风险领域，以确保完全遵守隐私条例
T0916	与隐私官，首席信息安全官，法律顾问和业务部门一起管理隐私事件和违规行为
T0917	与首席信息安全官协调，以确保安全和隐私惯例之间的一致性
T0918	建立，实施和维护组织范围的政策和程序，以遵守隐私条例
T0919	确保公司保持适当的隐私和保密通知，同意和授权表格和材料
T0920	制定和保持适当的沟通和培训，以促进和教育所有劳动者成员和董事会成员关于隐私合规问题和要求以及不遵守情事的后果
T0921	确定与组织机构的隐私计划相关的业务合作伙伴需求
T0922	建立和管理接收，记录，跟踪，调查和采取纠正措施的过程，适用于有关公司隐私政策和程序的投诉
T0923	与有关管理机构和其他法律实体以及组织机构干事合作进行合规审查或调查
T0924	执行正在进行的隐私合规监控活动
T0925	监督信息隐私技术的进步，以确保组织机构的采用和合规性
T0926	制定或协助开发隐私培训材料和其他沟通，以增加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了解
T0927	任命和指导一个 IT 安全专家团队
T0928	与主要利益相关者合作建立网络空间安全风险管理计划

A.5 NCWF 知识描述

表 6 提供了网络空间安全岗位从业人员需要具备的专业知识列表。这个列表中罗列的知识也被收录在附录 B 岗位角色的详细描述中。由于这些知识领域已经久经演化，并且将继续演化下去，所以并没有以特定的标准排序，而将以简单的方式按序号添加。

表格 6 NCWF 知识描述

ID	描述
K0001	计算机网络概念和协议，以及网络安全方法论知识
K0002	风险管理过程知识（比如评估和风险环境的方法）
K0003	与网络空间安全相关的国家和国际法律、规定、政策和道德要求知识。
K0004	网络空间安全原则知识
K0005	网络空间威胁和漏洞知识
K0006	网络空间安全漏洞对具体操作影响的知识。
K0007	认证、授权和访问控制的知识
K0008	客户组织机构业务流程和运作的知识
K0009	应用漏洞的知识
K0010	支持网络基础设施的通信方法、原则和概念知识（比如加密、双集线器、时分复用器）
K0011	网络设备的能力和适用范围的知识，包括集线器、路由器、交换机、网桥、传输介质和相关硬件。
K0012	能力分析和需求分析的知识
K0013	网络空间防御和漏洞评估工具的知识，包括开源工具和他们的能力。
K0014	复杂数据结构的知识
K0015	计算机算法的知识。
K0016	计算机编程原则的知识，比如面向对象的设计。
K0017	处理数字取证数据的概念和实践知识。
K0018	密码算法知识。（比如 IPSEC、AES、GRE、IKE、MD5、SHA、3DES）
K0019	密码学和密钥管理的概念知识。
K0020	数据管理和数据标准化政策和标准的知识。
K0021	数据备份、备份类型（比如全备份、增量备份）和数据恢复的概念和工具的知识。
K0022	数据挖掘和数据仓库原理知识。
K0023	数据库管理系统、查询语言、关系表和视图的知识。
K0024	数据库系统的知识
K0025	数字版权管理知识。
K0026	灾难恢复，业务持续性计划的知识。
K0027	组织机构企业信息安全架构系统的知识。
K0028	组织机构评估和验证需求的知识。
K0029	组织机构 LAN/WAN 路径的知识。
K0030	计算机架构中应用的电子工程的知识。包括电路板、处理器、芯片和相关的计算机硬件。
K0031	企业消息系统和相关软件的知识。

K0032	容错知识
K0033	主机/网络访问控制机制的知识（比如访问控制列表）。
K0034	了解网络服务和协议如何交互提供网络通信服务的知识。
K0035	系统组件如何安装、集成和优化的知识。
K0036	人机交互原理知识。
K0037	安全评估和授权流程知识
K0038	在使用、处理、存储和传输信息或数据中，管理相关风险的网络空间安全原则知识。
K0039	在软件开发中应用的网络空间安全原则和方法知识。
K0040	从警报、建议、勘误表和公告中了解已知漏洞
K0041	事件分类、事件响应和响应时间轴的知识。
K0042	事件响应和处理方法的知识。
K0043	业界标准活动或组织机构可接受的分析原则和方法知识。
K0044	网络空间安全原则和组织机构级需求知识（机密性、完整性、可用性、认证授权和不可抵赖性相关知识）
K0045	信息安全系统工程原理知识。
K0046	通过入侵检测技术来检测主机和网络入侵的相关方法和技术知识。
K0047	IT 架构概念和框架知识。
K0048	风险管理框架（RMF）要求知识
K0049	IT 安全原理和方法知识（比如防火墙、DMZ 区和加密）
K0050	包括带宽管理的局域网和广域网原则和概念知识。
K0051	低层次计算机语言的知识（比如汇编语言）
K0052	数学知识，包括对数，三角函数，线性代数，微积分，统计学。
K0053	系统性能和可用性的指标和度量知识。
K0054	评估、实施、IT 安全评估传播、监控、检测和使用标准化概念和能力进行修复的工具和过程的主流工业方法。
K0055	微处理器知识
K0056	网络接入、身份识别和访问管理知识（比如 PKI）
K0057	网络硬件设备和功能的知识
K0058	网络流量分析方法的知识
K0059	新兴的 IT 和网络空间安全技术的知识
K0060	操作系统知识
K0061	网络中流量如何流动的知识（比如 TCP、IP、OSI 模型、ITIL）
K0062	流量包分析的知识
K0063	并行和分布式技术的概念知识
K0064	性能调优工具和技术知识
K0065	基于策略的风险自适应访问控制知识
K0066	隐私影响评估知识
K0067	过程工程概念知识
K0068	编程语言结构和逻辑知识
K0069	比如 SQL 语言类似的查询语言知识
K0070	系统和应用安全威胁和漏洞的知识（比如缓冲区溢出、移动代码、跨站脚本、SQL 注入、竞争条件攻击、隐蔽信道、重放攻击、面向返回攻击、恶意代码）

K0071	远程访问技术概念知识
K0072	资源管理原则和技术知识
K0073	安全配置管理技术知识
K0074	安全管理中关键概念的知识（比如发版管理、补丁管理）
K0075	安全系统设计工具、方法和技术知识
K0076	服务器管理和系统工程理论、概念和方法知识。
K0077	服务端和客户端操作系统的知识
K0078	服务器诊断工具和容错技术的知识
K0079	软件调试原则的知识。
K0080	软件设计工具、方法和技术知识
K0081	软件开发模型知识（比如瀑布模型、螺旋模型）
K0082	软件工程知识
K0083	了解组织机构数据资产的来源、特征和用途。
K0084	结构化分析原则和方法知识
K0085	系统和应用安全威胁和漏洞知识。
K0086	包括自动化系统分析和设计工具在内的，系统设计工具、方法和技术知识。
K0087	了解系统设计相关的系统软件和组织机构设计标准、政策和授权方法的知识（比如 ISO 指南）
K0088	系统管理概念的知识
K0089	系统诊断工具和容错技术的知识
K0090	包括软件安全和可用性在内的，系统生命周期管理原则的知识。
K0091	系统测试和评估方法的知识
K0092	系统基础流程的知识
K0093	关键通信概念的知识（比如路由算法、光纤系统链路预算，多分复用）
K0094	各种互相关联的能够产生内容的技术的能力和功能知识（比如 wiki、社交网络、博客）
K0095	组织和管理信息的各种关联技术的能力和功能知识。（比如数据库、书签引擎）
K0096	各种协作技术的能力和功能知识（比如组件（groupware）、SharePoint）
K0097	物理和虚拟数据存储介质特征的知识。
K0098	了解网络防御服务提供商报告结构和其组织内部的处理流程
K0099	常用网络协议（比如 TCP/IP）、服务（比如 Web、Mail、DNS）以及他们如何交互，来实现网络通信的知识。
K0100	企业 IT 架构的知识
K0101	了解组织机构的企业 IT 目标知识
K0102	系统工程过程知识
K0103	确保设备功能正常运行，需要日常维护的类型和频率知识。
K0104	VPN 安全的知识
K0105	Web 服务知识，包括 SOA、SOAP 和 WSDL。
K0106	了解网络攻击构成要素的知识以及网络威胁和漏洞关系的知识。
K0107	内部威胁调查、报告、调查工具和法律/规定的经验和知识。
K0108	各种网络通信介质（计算机和电话网络、卫星、光纤和无线）的概念、数据和操作的知识
K0109	包括各种类型组件和外设（比如 CPU、网卡、数据存储）的功能在内的，物理

	计算机基本组件和架构的知识。
K0110	在指定的责任领域内（比如历史的国家特有的战术、技术和程序，新兴的能力），常见对手的战略、技术和程序
K0111	了解常见的网络工具（比如 ping\tracert\nslookup）和相关提示信息的解释
K0112	纵深防御的原则和网络安全的结构知识
K0113	不同类型的网络通信知识（比如 LAN、WAN、MAN、WLAN、WWAN）
K0114	电子设备的知识（比如计算机系统/组件、访问控制设备、数字相机、电子记事本、硬盘、内存、调制解调器、网络组件、打印机、可移动存储、扫描仪、电话、复印机、信用卡读卡器、传真机、GPS）
K0115	那些可能被对手利用的计算机新兴技术知识
K0116	文件扩展名（比如.dll, .bat, .zip, .pcap, .gzip）的相关知识
K0117	文件系统实现的相关知识（比如 NTFS、FAT、EXT）
K0118	获取和保存数字证据的过程知识（比如物证连续保存）
K0119	Windows 或 Linux/Unix 环境下的黑客攻击方法知识。
K0120	信息如何被需求以及信息如何在跨外部机构之间被转换、跟踪和设置优先顺序的知识。
K0121	信息安全程序管理和项目管理原则和技术的知识。
K0122	了解硬件、操作系统和网络技术调查研究的意义。
K0123	与（证据）采纳（比如联邦证据规则）相关的法律管理知识。
K0124	多个认知领域以及在每个认知领域学习时适用的工具和方法知识。
K0125	收集、打包、传输和存储电子证据，以避免（证据）改变、丢失、物理损坏或数据破坏的处理流程知识。
K0126	安全能力获得的知识（比如甲方技术代表职责、安全采购、供应链风险管理）
K0127	了解信息结构相关的性质和功能知识（比如国家信息基础设施）
K0128	持久化数据的类型和集合的相关知识
K0129	Unix 命令行的知识（比如 mkdir\mv\ls\passwd\grep）
K0130	虚拟化技术和虚拟机的开发和维护的知识
K0131	网络邮件收集、搜索/分析的技术、工具和 cooki 知识
K0132	哪些系统文件（比如日志文件、注册表文件、配置文件）包含相关信息，以及如何找到这些系统文件的知识。
K0133	数字取证数据的类型以及如何识别他们的知识。
K0134	移动取证知识
K0135	Web 过滤器技术知识
K0136	不同电子通信系统和方法的知识（比如 e-mail、VOIP、即时通讯、论坛、直接视频广播）
K0137	对已有网络系统范围的知识（比如 PBX, LANs, WANs, WIFI, SCADA）
K0138	Wi-Fi 知识
K0139	解释型和编译型计算机语言的知识
K0140	安全编码技术的知识
K0141	撤销，已融入 K0420
K0142	收集管理过程、能力和限制的知识
K0143	前端收集系统的知识，包括网络流量收集、过滤器和选择器。
K0144	全球化背景下，社会化动态计算机攻击的知识

K0145	安全事件关联工具的知识
K0146	了解组织机构的核心业务/使命流程知识
K0147	新兴的安全话题、风险和漏洞知识
K0148	进出口控制规则和责任机构的知识，以减少供应链风险
K0149	组织机构的风险承受能力和/或风险管理方法知识
K0150	企业事件响应程序、规则和职责知识
K0151	当前和新兴的威胁和微信向量的知识
K0152	了解 IT 安全原则和方法相关的软件知识（比如模块化、分层、抽象、数据隐藏、简化/最小化原则）
K0153	软件质量保障流程知识
K0154	供应链风险管理标准、过程和实践知识
K0155	电子证据法的知识
K0156	证据的法律规则和法庭程序的知识
K0157	网络防御政策、过程和法规的知识
K0158	组织机构 IT 用户安全政策知识（比如账户创建、密码规则和访问控制）
K0159	VoIP 的知识
K0160	网络层常见攻击向量的知识
K0161	不同攻击类别的知识（比如被动攻击、主动攻击、内部攻击、临近攻击、分布攻击）
K0162	不同操作威胁环境的知识（比如第一代的脚本小子，第二代的非国家支持黑客，第三代的国家支持的黑客）
K0163	关键的 IT 采购需求知识
K0164	功能、质量和安全需求以及他们如何应用到供应（元素和流程）的指定项中。
K0165	风险威胁评估知识
K0166	了解相关信息结构的性质和功能
K0167	了解基本的系统管理，网络和操作系统加固技术。
K0168	适用相关法律的知识（电子通信隐私法、外国情报监视法、保护美国法案、搜查扣押法案、公民自由和隐私法案），美国议会法案（比如法案编号 10、18、32、50），总统令、行政法规以及工作相关的行政刑事法规和程序
K0169	IT 供应链安全和风险管理策略、需求和程序的知识
K0170	当地特定系统需求的知识（比如那些因为安全、性能和可靠性原因，而没有使用标准信息技术的关键基础设施系统）
K0171	硬件逆向工程技术知识
K0172	中间件知识（比如企业服务总线和消息队列）
K0173	撤销，并入 K0499
K0174	网络协议知识
K0175	软件逆向工程技术知识
K0176	XML schema 知识
K0177	一般攻击阶段的知识（比如踩点扫描、枚举猜测、获取访问权限、特权提升、维持访问、网络渗透、轨迹隐藏）
K0178	安全软件开发方法、工具和实践知识
K0179	网络安全架构概念知识，包括拓扑、协议、组件和原理（比如应用纵深防御）
K0180	网络系统管理原理、模型、方法（比如端到端系统性能监控）和工具知识

K0181	传输记录（比如蓝牙、RFID、红外网络、Wi-Fi、寻呼、移动电话、卫星天线）和干扰技术（阻断不良信息或则阻止已安装系统正常运行）相关知识。
K0182	Data Carving 技术和工具（比如 Foremost）
K0183	逆向工程概念知识
K0184	反取证的策略、技术和程序知识
K0185	普通取证工具配置和支撑应用知识（比如 VMWare、Wireshark）
K0186	调试过程和工具知识
K0187	了解异常行为可能使用哪些不同类型文件的知识
K0188	恶意软件分析工具（比如 OD、IDA）知识
K0189	虚拟机觉察到的恶意软件，调试器觉察到的恶意软件以及打包 packing 的知识。
K0190	加密方法的知识
K0191	签名实施影响的知识
K0192	Windows/Unix 端口和服务的知识
K0193	数据库的数据修复高级安全特性知识
K0194	了解安全、治理、采购和管理相关的，基于云的知识管理技术和概念知识，
K0195	基于敏感性和其他风险因素的数据分类标准和方法知识
K0196	了解与密码技术和其他安全技术相关的进出口法规。
K0197	基于 Java 的数据库访问 API 接口知识（比如 JDBC）
K0198	组织机构过程提高概念和过程成熟度模型（比如 CMMI 开发模型、CMMI 服务模型和 CMMI 采购模型）
K0199	安全架构概念和企业构架构参考模型（比如 Zackman、FEA）
K0200	网络服务管理概念和相关标准（比如 ITIL）的知识
K0201	对称密钥轮转技术和概念知识
K0202	应用防火墙概念和功能知识。（例如单点认证/审计/策略执行，恶意内容扫描，PCI 和 PII 中的数据匿名，数据丢失保护扫描，加速密码操作，SSL、REST/JSON 处理等）
K0203	安全模型知识（比如 BLP 模型、BIBA 模型、Clark-Wilson 完整性模型）
K0204	评估技术知识（规则、评估计划、测试、测验）
K0205	基本的系统、网络和操作系统加固技术知识
K0206	道德黑客（白帽）的原则和技术知识
K0207	电路分析知识
K0208	基于计算机的培训和网络学习（E-Learning）服务知识
K0209	隐蔽通信的技术知识
K0210	数据备份和恢复的概念知识
K0211	机密性、完整性和可用性需求知识
K0212	网络空间安全软件产品知识
K0213	教学设计和评估模型知识（比如 ADDIE 模型、Smith/Ragan 史密斯/雷根模型，Gagne 教学事件、柯氏评估模式）
K0214	风险管理框架评估方法论知识
K0215	组织化的培训政策知识
K0216	学问分类水平知识（比如布鲁姆学问分类法）
K0217	学习管理系统以及它们在学习管理中使用的知识

K0218	学习形式的知识（比如同化、听觉和动觉）
K0219	局域网和广域网原理知识
K0220	学习模式的知识（比如死记硬背、观察学习）
K0221	OSI 模型和底层网络协议知识（比如 TCP/IP）
K0222	网络空间防御活动相关的法律、法定权利、限制和规定知识。
K0223	撤销，并入 K0073
K0224	Unix/Linux 和/或 Windows 操作系统的系统管理概念知识
K0225	部署在 CC/S/A 上的常用网络协议和服务知识
K0226	组织化培训系统知识
K0227	了解各种类型的计算机架构
K0228	分类学和语义本体理论知识
K0229	了解可以记录错误、异常和应用错误和日志的应用
K0230	云服务模型和事件响应的可能限制的知识
K0231	了解危机处理的协议、流程和技术
K0232	关键协议的知识（比如 IPSEC, AES, GRE, IKE）
K0233	NCWF、岗位角色和关联的任务、知识、技能和能力的知识
K0234	全领域网络空间能力的知识
K0235	知道如何利用政府研发中心、智库、高校研究机构和工业系统的知识。
K0236	了解如何利用 Hadoop，java、python，SQL，Hive，PIG 来探索数据。
K0237	了解服务台的行业最佳实践
K0238	机器学习理论和原理知识
K0239	交替使用书面的、口头的和视觉的方式，进行媒体制作、传播技术和方法
K0240	多层次/安全的跨域解决方案知识
K0241	组织机构的人力资源政策、流程和程序知识
K0242	组织机构的安全政策知识
K0243	组织机构的培训和教育政策、流程和程序知识
K0244	了解那些可能预示可疑或异常行为的身体或生理的行为活动。
K0245	进行培训和教育需求评估的原则和过程知识
K0246	相关概念、过程、软件、装备和技术应用的知识
K0247	客户支持服务相关的远程访问过程、工具和能力的知识
K0248	战略理论和实践的知识
K0249	可持续技术、过程和策略知识
K0250	测试评估流程知识
K0251	包括事实和证据的陈述在内的司法程序知识
K0252	培训和教育原则和方法的知识，从而进行课程设计、个人和小组教学指导、培训和教学效果评估。
K0253	撤销，并入 K0227
K0254	二进制分析的知识
K0255	包括拓扑、协议和组件在内的网络架构概念知识。
K0256	撤销，并入 K0224
K0257	IT 收购/采购需求知识
K0258	测试过程、原则和方法论知识（包括 CMMI）
K0259	恶意软件分析概念和方法知识

K0260	个人验证信息（PII）数据安全标准知识
K0261	支付卡行业数据安全标准（PCI DSS）知识
K0262	个人医疗信息（PHI）数据安全标准知识
K0263	IT 风险管理政策、需求和流程知识
K0264	包括 IT 供应链安全/风险管理政策、防篡改技术和需求在内的程序保护设计知识。
K0265	支撑 IT 安全性、性能和可靠性的基础设施知识。
K0266	如何评估供应商和/或产品可信度的知识
K0267	关键基础设施相关的法律、政策、流程或管理知识
K0268	法医（电子）足迹鉴别知识
K0269	移动通信架构知识
K0270	采购/收购生命周期过程的知识
K0271	操作系统结构和内部知识（比如进程管理、目录结构、已安装应用）
K0272	识别软件通信漏洞的网络分析工具知识
K0273	入侵链（Kill Chain）的一般知识（比如踩点扫描、枚举猜测、获取访问权限、特权提升、维持访问、网络渗透、轨迹隐藏）
K0274	传输记录（比如蓝牙、RFID、红外网络、Wi-Fi、寻呼、移动电话、卫星天线、VoIP）和干扰技术（阻断不良信息或则阻止已安装系统正常运行）相关知识。
K0275	配置管理技术知识
K0276	安全管理知识
K0277	当前和新兴的数据加密（比如列和表空间加密、文件和磁盘加密）、数据内置安全特性（包括内置密钥管理特性）的知识
K0278	数据库中当前和新兴的数据恢复安全特性知识
K0279	数据库访问编程接口知识（比如 JDBC）
K0280	系统工程理论、概念和方法知识
K0281	IT 服务目录知识
K0282	撤销，并入 K0200
K0283	跨平台（比如移动平台、PC、云）的协作和内容同步的用户用例知识
K0284	开发、应用用户凭证管理系统的知识
K0285	实现企业密钥托管系统支持静态数据（data-at-rest ）加密的知识
K0286	包括服务端和客户端操作系统的 N 层拓扑（网络）的知识
K0287	组织机构的信息分类程序和信息破坏处理程序知识
K0288	行业标准的安全模型知识
K0289	系统/服务器诊断工具和故障识别技术的知识
K0290	系统安全测试和评估方法的知识
K0291	包括基线和目标架构在内的企业 IT 架构概念和模式知识。
K0292	针对突发事件、问题和大事件管理的操作和处理流程知识
K0293	将组织机构的目标整合到（组织机构）架构的知识。
K0294	保持设备功能正常使用所需的 IT 系统运行、维护和安全知识
K0295	机密性、完整性、可用性原理知识
K0296	了解集线器、路由器、交换机、网桥、服务器、传输介质和相关硬件等网络设备的能力、适用范围和潜在漏洞知识。
K0297	对已确认安全风险的应对措施设计知识

K0298	对已确认安全风险的应对措施知识
K0299	确定一个安全系统如何工作（包括它的韧性和可靠性能力），以及条件、操作或环境变化将如何影响系统输出的知识。
K0300	网络映射和重建网络拓扑的知识
K0301	使用合适工具（比如 Wireshark, tcpdump）进行数据包层次分析的知识
K0302	计算机基本操作的知识
K0303	使用子网工具的知识
K0304	处理数字取证数据的基本概念和实践知识。
K0305	加密算法、信息隐写（stenography）和其他数据隐藏的形式知识
K0306	基础的物理计算机组件和架构的知识
K0307	常用网络工具的知识（比如 Ping\traceroute\nslookup）
K0308	密码学知识
K0309	那些可能被对手利用的新兴技术的知识
K0310	黑客方法论的知识
K0311	可用于识别技术趋势的行业指标知识
K0312	包括法定权利和限制在内的情报原则、政策和流程知识
K0313	外部组织机构和科研机构在网络空间（研究）关注点的知识（比如网络空间课程/培训和研发）
K0314	行业技术知识以及他们影响渗透/漏洞的区别。
K0315	信息收集和生产、汇报和信息共享方面的原则方法、过程和技术知识
K0316	民用或军用作战计划、作战计划概念、命令、政策和交战规则的知识
K0317	记录、查询已报告的偶发事件、问题和大事件的流程知识
K0318	操作系统命令行/提示符的知识
K0319	技术交付的能力和他们局限的知识
K0320	组织机构的评估和验证标准的知识
K0321	计算机架构和相关硬件/软件的（系统）工程概念知识
K0322	嵌入式系统的知识
K0323	系统容错方法论的知识
K0324	入侵检测系统 IDS/入侵防御系统 IPS 的工具和应用知识
K0325	信息论知识（比如源编码、信道编码、算法复杂度理论和数据压缩）
K0326	网络空间方法的知识，比如防火墙、DMZ 区和加密
K0327	包括带宽管理在内的局域网（LAN）、广域网（WAN）和企业（网）的原理和概念知识。
K0328	数学知识，包括对数，三角函数，线性代数，微积分，统计学和运营数据分析。
K0329	统计学知识
K0330	可以发现不常见和更复杂系统问题解决方案的能力知识
K0331	网络协议知识（比如 TCP、IP、DHCP、目录服务（比如 DNS））
K0332	网络协议知识，比如 TCP/IP、动态主机配置（DHCP？）、DNS 和目录服务
K0333	网络设计流程知识，包括理解安全目标、运营目标以及两者的权衡。
K0334	网络流量分析知识（工具、方法、流程）
K0335	当前和新兴的网络空间技术知识
K0336	访问身份认证方法的知识
K0337	撤销，并入 K0007

K0338	数据挖掘技术的知识
K0339	如何使用网络分析工具确认漏洞的知识
K0340	网络中流量如何流动的知识（比如 TCP、IP、OSI 模型）
K0341	网络空间安全相关的进出口控制法规和外部信息披露政策知识
K0342	渗透测试原理、工具和技术知识
K0343	本质原因分析技术知识
K0344	威胁环境知识
K0345	网络空间攻击者知识（比如脚本小子、内部威胁、非国家支持黑客、国家支持黑客）
K0346	集成系统组件的原理和方法知识
K0347	业务设计的知识和理解
K0348	了解广泛的基本通信介质概念和术语（比如计算机和电信网络、卫星、电缆、无线）
K0349	了解与网站相关的广泛概念（比如网站类型、管理、功能、软件系统等等）
K0350	公认的组织规划系统知识
K0351	管理网络空间目标和渗透利用的适用法规、法律、规定和政策。
K0352	各种形式的情报支持需求、话题和关注领域的知识
K0353	可能导致（信息）收集管理授权发生变化的所有情况的知识
K0354	所有报告和传播过程相关的知识
K0355	所有来源报告和传播过程的知识
K0356	分析工具和技术的知识
K0357	分析构建（内容分析法的第三个要素 analytical construct）和他们在业务环境评估中使用的知识
K0358	分析标准和（设置）情报置信水平目的知识
K0359	经过批准的情报传播过程的知识
K0360	汇编代码的知识
K0361	资产可用性、能力和限制的知识
K0362	攻击方法和技术的知识（DDoS、暴力、欺骗等等）
K0363	审计和日志处理的知识（比如基于服务器的日志）
K0364	评估（信息）采集任务所需的可用数据库和工具知识
K0365	包括不同类型的备份（比如全备份、增量备份）在内的，基本备份和恢复过程知识。
K0366	包括各种外设的功能在内的，基本计算机组件和架构知识。
K0367	基本的网络空间（攻击）操作活动的概念（比如踩点、扫描和枚举，渗透测试，黑/白名单）
K0368	基本的移植（扩散）知识
K0369	恶意活动的概念知识（比如踩点、扫描和枚举）
K0370	包括各种组件和外设（比如 CPU、网卡、数据存储）功能在内的基本的物理计算机组件和架构知识。
K0371	（信息）收集过程中的基本原理知识。（比如被叫号码识别，社交网络分析）
K0372	基本的编程概念知识（比如层次、结构、编译型 vs 解释型语言）
K0373	基本的软件应用（比如数据存储和备份、数据库应用）和他们漏洞的知识
K0374	现代数字和电话网络基本结构、架构和设计的知识

K0375	包括各类无线应用漏洞在内的基本无线应用的知识
K0376	包括信息需求、目标、结构和能力等等在内的，内外部客户和合作伙伴机构的知识。
K0377	标签标准、政策和流程的分类与控制知识
K0378	标签标准的分类和控制知识
K0379	包括信息需求、目标、结构和能力等等在内的，客户组织机构知识
K0380	协作工具和环境的知识
K0381	附带损害和影响评估的知识
K0382	（信息）收集能力和限制的知识
K0383	了解（信息）收集能力、访问、性能规格和限制的知识，满足收集计划（的要求）。
K0384	（信息）收集管理功能的知识（比如职位、职能、职责、产品、报告要求）
K0385	撤销，并入 K0142
K0386	（信息）收集管理工具的知识
K0387	（信息）收集计划流程和收集计划的知识
K0388	搜索/分析技术和工具（信息）收集的知识，包括聊天/好友列表,新兴技术、VIOP、基于 IP 的媒体（Media Over IP）、VPN、卫星小数据站 VSAT/无线、网络邮件和 cookie 等
K0389	传统的或非传统的（信息）收集来源的知识。
K0390	（信息）收集策略的知识
K0391	（信息）收集系统、能力和流程的知识
K0392	常见的计算机/网络感染（病毒、木马等）和感染方法（端口、附件等）的知识
K0393	常见的网络设备及其配置的知识
K0394	常见的数据库和数据库工具报告的知识
K0395	计算机网络基础知识（比如网络的基本计算机组件，网络类型等）
K0396	包括计算机语言、编程、测试、调试和文件类型在内的计算机编程概念知识，
K0397	操作系统的概念知识（比如 Linux、Unix）
K0398	网站相关的概念知识（比如 Web 服务/网页、主机、DNS、注册、类似 HTML 的 Web 语言）
K0399	危机行动计划和时间敏感型计划程序的知识
K0400	网络空间运营的危机行动计划知识
K0401	（信息）收集产品评估标准的知识
K0402	网络空间领域的目标选择和适用性的关键和漏洞条件（比如价值、恢复、隔离、对策）
K0403	密码的能力、限制和对网络空间操作的作用知识
K0404	当前（信息）搜集需求的知识
K0405	当前计算机入侵汇总的知识
K0406	主动防御和系统加固方面，主流的软件和方法知识
K0407	客户信息需求的知识
K0408	网络空间行动（比如网络防御、信息收集、环境准备、网络攻击）、原理、能力、限制和效果的知识
K0409	网络空间情报/信息收集能力和知识库的知识
K0410	网络空间法律和他们对网络空间规划影响的知识

K0411	网络空间法律、法规和他们对网络空间规划影响的知识
K0412	网络空间词汇/术语的知识
K0413	网络空间运营目标、策略和法律的知识
K0414	网络空间运营支持或启用流程的知识
K0415	网络空间运营术语/词汇的知识
K0416	网络空间运营的知识
K0417	数据通信技术知识（比如网络协议、以太网、IP、加密、光学设备、可移动介质）
K0418	终端或环境收集的数据流知识
K0419	数据库管理和维护知识
K0420	数据库理论知识
K0421	数据库、门户网站和相关传播工具的知识
K0422	解决冲突问题的步骤和程序的知识
K0423	包括与外部机构互动的解决冲突问题汇报的知识
K0424	拒绝和欺骗的技术知识
K0425	包括下属、横向部门和上级在内的，包括所有层级不同组织机构目标的知识
K0426	动态目标和蓄意目标的知识
K0427	加密算法和网络空间能力/工具的知识（比如 SSL、PGP）
K0428	WLAN 加密算法和工具的知识
K0429	企业级的信息管理知识
K0430	规避策略和技术的知识
K0431	不断发展/新兴的通信技术知识
K0432	了解网络空间运营策略、政策和机构相关的已有的、新兴的和长期的话题
K0433	了解对操作系统结构和操作进行取证的含义
K0434	包括流量收集、过滤和选择在内的前端收集系统知识
K0435	基础的网络空间概念、原则、限制和效果知识
K0436	基本的网络空间操作概念、术语/词汇（比如环境准备、网络攻击、网络防御）、原则、能力、限制和效果的知识
K0437	一般的 SCADA 系统组件知识
K0438	移动通信全球系统（GSM）架构的知识
K0439	管理目标的知识
K0440	基于主机的安全产品以及他们如何影响渗透利用和漏洞的知识
K0441	了解贯穿整个企业的信息和信息搜集需求是如何转换、跟踪和排定优先级的。
K0442	了解融合技术是如何影响网络空间操作的（比如数字技术、电信技术、无线技术）
K0443	了解集线器、交换机、路由器是如何在网络设计中一起工作的。
K0444	互联网应用如何工作的知识（SMTP 邮件、Web 邮件、聊天客户端、VOIP）
K0445	了解现代数字和电信技术网络如何影响网络操作的。
K0446	了解现代无线通信系统如何影响网络操作的
K0447	如何从元数据（比如 email、http）中，收集、查看和识别感兴趣目标的关键信息。
K0448	如何建立资源优先级的知识。
K0449	如何提取、分析和使用元数据的知识

K0450	撤销，并入 K0036
K0451	识别和报告流程的知识
K0452	可以提供 radius 认证和登录、DNS、邮件、Web 服务、FTF 服务、DHCP、防火墙和 SNMP 服务的 Unix 和 Windows 系统的知识。
K0453	指标和警告的知识
K0454	信息需求的知识
K0455	了解信息安全概念、以及对技术和方法促进
K0456	情报的能力和局限性的知识
K0457	情报密级的知识
K0458	情报学科知识
K0459	情报使用需求的知识（比如逻辑的需求、通信支持需求、可操作性需求、法律限制需求等）
K0460	环境和类似处理的情报准备知识
K0461	情报成产过程的知识
K0462	情报汇报的原则、政策、过程和媒介知识，包括汇报格式、汇报标准（需求和优先级）、传播情况和法律规定和限制。
K0463	情报需求任务系统的知识
K0464	可以支持计划、执行和评估的情报知识
K0465	内部和外部合作伙伴网络操作能力和工具的知识
K0466	内部和外部合作伙伴情报处理和关键信息和信息需求发展的知识
K0467	内部和外部合作伙伴组织机构能力和局限的知识（包括执行任务、收集、处理、利用和传播职责）
K0468	了解内部和外部合作伙伴的报告
K0469	对威胁能力和行为进行预演和/或模拟的内部行动的知识
K0470	互联网和路由协议的知识
K0471	互联网网络地址知识（IP 地址、无类域间路由、TCP/UDP 端口号）
K0472	入侵检测系统和签名（技术）的发展
K0473	入侵（规则）集的知识
K0474	关键网络威胁行为和他们构成的知识
K0475	操作环境和威胁关键因素的知识
K0476	语言处理工具和技术的知识
K0477	了解领导的意图和目标。
K0478	有针对性的法律考虑知识
K0479	恶意软件分析和特征化的知识
K0480	恶意软件的知识
K0481	检查各种漏洞利用行为的方法和技术知识
K0482	弄清所收集资产的情况和可用性的方法知识
K0483	了解从所有潜在来源收集和汇总信息的方法
K0484	中点收集的知识（过程、目标、机构和对象等）
K0485	网络管理的知识
K0486	网络构建和网络拓扑的知识
K0487	网络安全的知识（比如加密、防火墙、认证、蜜罐、边界保护）
K0488	网络安全实现的知识（比如基于主机的 IDS、IPS、访问控制列表），包括他们

	的功能以及在网络中的位置
K0489	网络拓扑的知识
K0490	撤销，并入 K0058
K0491	网络和互联网通信原理知识（比如设备、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、操作系统等等）
K0492	非传统的（信息）收集方法知识
K0493	混淆隐藏技术的知识（比如 TOR/Onion/匿名者，VPN/VPS，加密）
K0494	了解目标、形式、操作环境以及内部外部合作伙伴的（信息）收集能力的状态
K0495	现在的和未来的（网络空间）运营知识
K0496	（网络空间）运营资产约束的知识
K0497	（网络空间）运营效果评估的知识
K0498	（网络空间）运营计划流程知识
K0499	（网络空间）运营安全的知识
K0500	机构和/或合作伙伴（信息）收集系统能力和流程的知识（比如收集和协议处理）
K0501	组织机构网络空间运营程序、策略和资源的知识
K0502	组织机构决策支持工具和/或方法的知识
K0503	了解资源和资产就绪报告的组织形式，以及它的运营相关性和对情报收集的影响。
K0504	了解网络空间的组织机构问题、目标和运营（情况），以及管理网络空间运营的法规和政策命令。
K0505	了解组织机构目标和收集管理中的相关需求。
K0506	了解组织机构目标、领导力优先级和决策风险
K0507	了解组织机构或合作伙伴对数字网络的利用
K0508	了解与内部和/或外部机构合作的组织机构政策和计划概念
K0509	了解组织机构和合作伙伴的权利、职责和对实现目标的贡献。
K0510	了解组织机构和合作伙伴的政策、工具、能力和过程。
K0511	了解组织机构层级和网络空间决策过程
K0512	了解组织机构计划的概念
K0513	了解组织机构的优先事项、法定权力和需求提交流程。
K0514	了解组织机构的组成结构和相关情报能力
K0515	OSI 模型和底层网络协议（比如 TCP/IP）的知识
K0516	包括集线器、交换机、路由器、防火墙等在内的物理的和逻辑的网络设备和基础设施知识。
K0517	PIR 审批流程知识
K0518	对活动启动进行规划的知识
K0519	规划有适应性的时间表、危机行动和时效性计划。
K0520	了解目标仿真相关的原则和实践，比如目标的知识学习、关联和联系、通信系统和基础设施。
K0521	了解优先级信息，包括它如何产生、在哪里发布、如何访问等等。
K0522	产品利用和传播需求和架构的知识
K0523	主流厂商的产品和系统命名知识）（比如安全套件厂商-趋势科技、 Symantec, McAfee, Outpost, Panda, Kaspersky），以及他们对渗透利用/漏洞影响的区别。

K0524	相关法律、规定和政策知识
K0525	与网络空间运营计划相关的情报计划产品知识
K0526	研究策略和知识管理的知识
K0527	风险管理和缓解策略知识
K0528	基于卫星的通信系统知识
K0529	脚本知识
K0530	包括在渗透利用中影响的网络组件在内的，安全软硬件选项知识，
K0531	软件配置的安全含义的知识
K0532	转移目标语言的知识（比如缩写、行话、技术术语、密语）
K0533	特定的目标识别和他们用法的知识
K0534	人员管理、（任务）分派和（物资）分配流程的知识
K0535	目标研究的策略和工具的知识
K0536	渗透利用工具（比如 sniffer、keylogger）的结构、方法和策略知识，以及相关技术（比如获取后门权限、收集/导出数据、对网络中的其他系统进行漏洞分析）的知识
K0537	Unix/Linux、Windows 操作系统系统管理概念的知识（比如进程管理、目录结构、已安装应用、访问控制）
K0538	了解目标和威胁的组织结构、关键能力和关键漏洞的知识
K0539	目标通信系统的配置和他们关键元素的知识（比如目标的关联、活动和通信基础设施）
K0540	目标通信工具和技术的知识
K0541	目标的文化、方言、表述、习惯语和省略语的知识
K0542	目标发展的知识（比如概念、角色、职责、产品等等）
K0543	预估的目标维修和恢复时间的知识
K0544	目标情报收集和操作准备的技术和生命周期的知识
K0545	目标语言知识
K0546	目标列表发展的知识（比如 RTL, JTL, CTL 等等）
K0547	目标方法和过程的知识
K0548	目标或威胁的网络空间参与者和程序
K0549	了解目标审核和验证程序
K0550	目标的知识，包括当前相关的事件、通信配置、参与者、历史（语言和文化）和参考框架。
K0551	目标周期的知识
K0552	任务机制的知识
K0553	对系统的和下级的（信息/情报）收集资产的任务处理知识
K0554	了解任务、收集、处理、利用和传播的知识
K0555	TCP/IP 网络协议的知识
K0556	电信基础的知识
K0557	终端或环境（信息）收集的知识（过程、目标、组织结构、靶标等等）
K0558	与搜集需求和搜集管理相关的可用工具和应用知识
K0559	融合应用（converged application）的基本结构、架构和设计的知识
K0560	现代通信网络的基本结构、架构和设计的知识
K0561	基本网络安全的知识（比如加密、防火墙、认证、蜜罐、边界保护）

K0562	了解新兴（信息）收集能力、访问方式和/或流程的能力和局限性。
K0563	在应用到规划中的网络空间行动时，这些内部和外部（信息）收集能力、局限性和任务处理方法知识。
K0564	目标通信网络的特征知识（比如容量、功能、路径、关键节点）
K0565	常用的网络和路由协议（比如 TCP/IP）、服务（比如 Web、邮件、DNS），以及他们如何交互来提供网络通信服务的知识。
K0566	关键信息需求以及计划如何使用使用的知识
K0567	从（信息）收集原点到知识仓库和工具的数据流知识
K0568	（信息）收集管理定义和收集管理权限的知识
K0569	现有的任务、收集、处理、利用和传播架构的知识
K0570	可能影响（信息）收集业务的威胁因素的知识。
K0571	在收集处理中的反馈周期知识
K0572	了解模拟威胁行为帮助组织机构（提升安全）的内部团队的能力
K0573	数字取证的基础知识，以便提取发现有用的情报。
K0574	了解语言分析对网内业务功能的影响
K0575	了解内部和外部合作伙伴人员评估的影响
K0576	信息环境的知识
K0577	情报框架、流程和相关系统的知识
K0578	情报需求开发和信息处理要求的知识
K0579	了解上级、下级和平级机构的结构、角色和职责
K0580	了解组织机构已经建立的（信息）收集计划的格式
K0581	了解组织机构的计划、运营和目标周期。
K0582	了解组织规划和人员编制流程
K0583	了解反映（组织机构）目标的组织规划/指令/指南
K0584	了解临时交接（信息）收集授权的机构政策/流程。
K0585	包括功能、职责以及内部主要模块之间相互关系在内的，网络空间运营相关的所有组织结构知识。
K0586	行为和练习分析科目的输出结果知识
K0587	需要建立环境准备和关注产品所需的 POC、数据库、工具和应用的知识。
K0588	了解下级、平级的和上级机构的信息需求优先级知识
K0589	评估业务绩效和影响的流程知识
K0590	了解与关键信息需求处理同步的业务评估程序。
K0591	产品职责、有机分析（rganic analysis）和产品能力的知识
K0592	了解目标模板的（建设）目的和贡献者
K0593	了解网络空间运营的范围和他们潜在的情报支持需求、问题和关注点。
K0594	结束状态、目标、效果和操作序列等等之间关系的知识
K0595	了解操作目标、情报需求和情报产品任务之间关系
K0596	了解信息处理的要求
K0597	了解网络空间运营在支撑和促进其他机构运营上的作用。
K0598	了解组织机构特定计划、指南和授权的意图和结构
K0599	了解现代数字和电话网络的结构、架构和设计。
K0600	了解现代无线通信系统的结构、架构和设计
K0601	了解用于协作的系统/架构/通信知识

K0602	了解各种（信息）收集的科目和能力
K0603	了解目标或威胁使用互联网的方式
K0604	威胁和/或目标系统的知识
K0605	了解（情报）引爆、提示、混合和冗余的知识
K0606	了解转录的发展过程和技术（比如一字不差转录、主旨转录、总结转录）
K0607	了解翻译的过程和技术
K0608	Unix、Linux 和 Windows 操作系统的结构和内部知识（比如进程管理、目录结构、已安装应用）
K0609	虚拟机技术的知识
K0610	虚拟化产品（VMWare、虚拟 PC）的知识
K0611	撤销，并入 K0131
K0612	了解什么构成了网络的“威胁”
K0613	了解组织机构的运营规则者是谁，怎样、在哪里能够联系他们，他们的期望是什么。
K0614	包括现代无线通信系统的基本结构、架构和设计在内的，无线技术的知识（比如蜂窝、卫星、GSM）

A.6 NCWF 技能描述

表 7 提供了网络空间安全岗位从业人员需要具备的专业技能列表。这个列表中罗列的技能也被收录在附录 B 岗位角色的详细描述中。由于这些技能已经久经演化，并且将继续演化下去，所以并没有以特定的标准排序，而将以简单的方式按序号添加。

表格 7 NCWF 技能描述

ID	描述
S0001	在安全系统中进行漏洞扫描、识别漏洞的技能
S0002	在数据管理系统设计中，分配存储容量的技能
S0003	识别、捕获、控制和汇报恶意软件的技巧
S0004	分析网络流量能力和性能特征的技能
S0005	将合适的信息技术应用到推荐的解决方案中的技巧
S0006	应用保密性、完整性和可用性原则的技巧
S0007	应用主机/网络访问控制的技巧（比如访问控制列表）
S0010	应用特定组织机构的系统分析原则和技术的技能
S0009	评估安全系统和设计健壮性的技能
S0010	进行能力和需求分析的技能
S0011	进行信息搜索的技能
S0012	构建知识图的技能（比如知识库图）
S0013	进行查询和开发分析数据结构算法的技能
S0014	进行软件调试的技能
S0015	进行测试活动的技能
S0016	配置和优化软件的技能
S0017	创建和使用数据或统计模型的技能
S0018	具备技能可以创建反映系统安全目标的策略

S0019	能够创建程序来验证和处理多个输入数据的技能。这些输入包括命令行参数、环境变量和输入流。
S0020	开发和部署签名（程序）的技能
S0021	设计数据分析结构的技能（比如你测试必须生成的数据类型，以及你如何分析这些数据）
S0022	设计对策，识别安全风险的技能
S0023	基于网络空间安全原则设计安全控制的技能。
S0024	设计软硬件结合方案的技能
S0025	通过入侵检测技术（比如 snort）来检测主机和网络入侵事件的技能。
S0026	对于给定系统，确定合适的测试要求水平的技能
S0027	确定一个安全系统如何工作（包括它的弹性和可靠性能力），以及条件、操作或环境变化将如何影响系统输出。
S0028	开发数据字典的技能
S0029	开发数据模型的技能
S0030	开发基于操作的测试场景的技能
S0031	开发和应用安全系统访问控制的技能
S0032	开发、测试和实现网络基础设施应急和恢复计划的技能
S0033	诊断连接性问题的技能
S0034	识别信息系统和网络的保护需求（比如安全控制）的技能
S0035	建立路由 schema 的技能
S0036	评估安全设计是否充分的技能
S0037	生成查询和报告的技能
S0038	识别系统性能的度量方法和指标，为了提高或改善系统目标相关的性能指标，识别需要采取的行动。
S0039	识别系统性能下降的可能原因，并采取行动来减轻这种下降的技能。
S0040	实施、维护和改进网络安全措施的技能
S0041	安装、配置和解决 LAN 和 WAN 组件文件的技能，比如路由器、集线器和交换机。
S0042	维护数据库的技能
S0043	维护目录服务的技能
S0044	模仿威胁行为的技能
S0045	优化数据库性能的技能
S0046	使用合适工具进行数据包层面的分析的技能（比如 Wireshark, tcpdump）
S0047	遵循标准程序或国家标准，保存证据完整性的技能
S0048	系统集成测试的技能
S0049	测量和汇报智力资本的技能
S0050	设计模型和构建用例图的技能（比如 UML 语言）
S0051	使用渗透测试工具和技术的技能
S0052	使用社工技术的技能
S0053	传感器调优技能
S0054	使用事件处理方法论的技能
S0055	使用知识挂了技术的技能
S0056	使用网络管理工具分析网络流量模式的技能（比如 SNMP）
S0057	使用协议分析器的技能

S0058	使用合适工具修复软件、硬件和系统外设的技能
S0059	使用 VPN 设备和加密技术的技能
S0060	使用当前主流的编程语言（比如 Java、C++）编写代码的技能
S0061	编写测试计划的技能
S0062	分析内存 Dump 提取信息的技能
S0063	从多种网络防御资源收集数据的技能
S0064	开发和执行技术培训程序和课程的技能
S0065	在多个介质中识别和提取法医感兴趣数据的技能（比如介质取证）
S0066	识别技术能力差距的技能
S0067	在 Windows、Unix、Linux 内识别、修改和操纵合适的系统组件的技能。（比如密码、用户账号、文件）
S0068	收集、打包、传输和存储电子证据，以避免（证据）改变、丢失、物理损坏或数据破坏的技能。
S0069	配置建立取证工作站的技能
S0070	与他人沟通有效传达信息的技能
S0071	使用取证工具套件的技能（比如 EnCase, Sleuthkit, FTK）
S0072	使用科学规则和方法解决问题的技能
S0073	使用虚拟机的技能
S0074	物理拆卸电脑的技能
S0075	在多个操作系统环境中进行取证分析的能力（例如，移动设备系统）。
S0076	配置和使用基于软件的计算机保护工具的技能（例如，软件防火墙、防病毒软件、反间谍软件）
S0077	保护网络通信的技能
S0078	识别和分类各种攻击与漏洞的类型的技能
S0079	保护网络免受恶意软件攻击的技能
S0080	进行危险评估的技能
S0081	利用网络分析工具识别漏洞的技能
S0082	评估测试计划的适用性和完整性的技能
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能
S0084	配置和使用网络保护组件的技能（例如，防火墙、VPN、网络入侵检测系统）
S0085	对技术系统进行审计或审查的能力
S0086	评估供应商或产品的可信度的技能
S0087	对于捕获的恶意代码进行深度分析的技能（例如，恶意软件取证）
S0088	使用二进制分析工具的技能（例如，Hexedit，命令编码机制，hexdump）
S0089	掌握单向散列函数的技能（例如，安全散列算法（SHA），消息摘要算法[MD5]）
S0090	分析异常代码是恶意或良性的技能
S0091	分析不稳定数据的技能
S0092	识别混淆技术的技能
S0093	根据调试器的结果以确定策略、技术和程序的技能
S0094	阅读十六进制数据的技能
S0095	识别通用的编码技术的能力（例如，异或[XOR]，美国信息交换用[ASCII]，Unicode，base64，Uuencode 标准代码，统一资源定位器[URL]编码）
S0096	阅读和解释签名的能力（例如，Snort）

S0097	应用安全控制的技能
S0098	通过入侵检测技术检测主机和基于网络的入侵的技能。
S0099	确定一个安全系统应该如何工作，以及什么样的条件、操作或环境的变化将如何影响这些结果的技能
S0100	使用和开发学习相关的活动（例如，剧本，教学游戏，互动练习）
S0101	使用工具进行（例如，宽频，网站，电脑，投影仪）教学的技能
S0102	应用技术交付的能力
S0103	评估预测能力和后续一个通用模型的技能
S0104	进行测试以及准备复查的能力
S0105	数据挖掘技术的能力
S0106	数据预处理的技能（例如，归责，还原,规范化、转换、提取、过滤、）
S0107	设计和记录整个程序测试和评估策略的能力
S0108	发展员工和职位资格标准的能力
S0109	识别隐藏的模式或关系的能力
S0110	识别测试和评估基础设施（人、范围、工具、仪器仪表）的要求的能力
S0111	与客户沟通对接的能力
S0112	管理测试资产、测试资源和测试人员以确保测试事件的有效完成的技能
S0113	执行格式转换以创建数据的标准表示形式的能力
S0114	执行敏感性分析的技能
S0115	准备测试和评估报告的能力
S0116	设计多级安全/跨领域解决方案的能力
S0117	提供测试和评价资源估计的技能
S0118	开发适用于机器语言的技能
S0119	回归分析的能力（例如，分层逐步，广义线性模型，普通最小二乘法，基于树的方法，物流）。
S0120	审查日志识别过去入侵证据的技巧的技能
S0121	系统、网络和操作系统硬化技术方面的技能
S0122	使用设计方法的技能
S0123	转换分析（例如，聚合，浓缩，处理）的技能
S0124	通过方案决议等，解决和诊断网络防御基础设施异常的技能
S0125	使用基本的描述性统计和技术的技能（例如，正态分布，模型分布，散点图）
S0126	使用数据分析工具的技能（如 Excel，Stata SAS，SPSS）。
S0127	使用数据映射工具的技能
S0128	使用人力和人事 IT 系统的技能
S0129	使用异常识别和清除技术的技能
S0130	使用 R，Python，PIG，HIVE，SQL 等编写脚本的技能
S0131	分析恶意软件的技能
S0132	进行位分析的技能
S0133	处理数字证据，包括保护和制作合法的、可靠的证据副本的能力
S0134	进行系统评估的技能
S0135	安全测试计划设计的技能(例如.单元、集成系统、验收)。
S0136	网络系统管理原则、模型、方法(如端到端系统性能监控)和工具的使用技能。
S0137	进行应用漏洞评估的技能

S0138	使用公共密钥基础设施（PKI）的加密和数字签名功能的应用程序（例如，S / MIME 邮件，SSL 流量）的技能
S0139	应用安全模型（如 Bell LaPadula 模型，Biba 完整性模型、Clark Wilson 的完整模型）的使用技能
S0140	把控应用系统工程过程的技能。
S0141	安全系统设计评估的技能
S0142	进行客户级问题的故障排除研究的技能
S0143	进行系统/服务器规划，管理和维护的技能
S0144	修正影响系统/服务器性能的物理和技术问题的技能
S0145	整合和应用符合系统安全目标的政策的技能
S0146	制定政策,使系统满足性能目标(如交通路由、SLA 的 CPU 规范)的技能
S0147	基于网络空间安全原则和信条的安全控制评估的技能
S0148	设计技术流程与解决方案的整合，包括系统与现代编程语言的技能
S0149	开发可以生成运维日志，处理错误,异常以及应用程序错误和日志记录的程序的技能。
S0150	实施和测试网络基础设施应急和恢复计划的技能。
S0151	排除故障的系统组件的技能（例如，服务器）
S0152	将操作需求转化为保护需求的技能（即安全控制）。
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	安装系统和组件升级的技能
S0155	监控和优化系统/服务器性能的技能
S0156	具有数据包分析的的技能（例如，wireshark tcpdump，等）。
S0157	恢复失败的系统/服务器的技能
S0158	操作系统管理的技能
S0159	按照符合批准的标准/或规范配置和验证网络工作站和外围设备的技能。
S0160	使用设计建模的技能（例如，统一建模语言）
S0161	撤销，合并到 S0160
S0162	构建子网的技能
S0163	撤销，合并到 S0060
S0164	评估应用程序的加密标准的技能
S0165	电子证据收集、包装、运输和存储避免变更、损失,物理伤害等破坏数据的技能。
S0166	识别技术交付能力上的差距的技能
S0167	识别安全系统中的漏洞的技能
S0168	使用应用网络空间安全方法的技能，如防火墙、加密等。
S0169	进行趋势分析的技能
S0170	配置和使用计算机保护组件的技能（如硬件防火墙、服务器、路由器等）。
S0171	执行影响/风险评估的技能
S0172	应用安全编码技术的技能
S0173	使用安全事件相关工具的技能
S0174	使用代码分析工具的技能
S0175	执行根本原因分析的技能
S0176	管理计划的活动，包括准备功能和具体的支持计划，准备，管理通信和编制程序的技能。

S0177	目标通信网络分析的技能
S0178	分析重要的网络数据的技能（例如，路由器配置文件，路由协议）。
S0179	分析语言处理工具以提供反馈以促进工具开发的技能
S0180	撤销，合并到 S0062
S0181	分析数据收集点的技能
S0182	通过无线局域网分析目标收集的内部和外部通信的技能
S0183	分析终端或环境收集到的数据的技能
S0184	分析流量以识别网络设备的技能。
S0185	使用应用分析方法，通常用于支持规划和证明建议的策略和行动的过程的技能。
S0186	应用紧急规划的程序的技能。
S0187	应用各种分析方法，工具和技术的技能（例如，相互竞争的假设；推理链；场景方法；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，Delphi 和模式分析）
S0188	评估目标的参考框架的技能（例如，动机，技术能力，组织结构，敏感性）。
S0189	评估或估计在网络空间运营期间和之后网络操作产生的影响的技能。
S0190	评估现有的工具，以确定需要改进的技能
S0191	评估现有的分析工具在各种情况下的适用性的技能
S0192	审计防火墙、路由器、和入侵检测系统的技能
S0193	遵守目标信息的法律限制的技能
S0194	进行 non-attributable 无主研究的技能
S0195	使用所有可用的资源进行研究的技能
S0196	利用深层网络进行研究的技能
S0197	进行社交网络分析，好友列表分析，或 cookie 分析的技能。
S0198	进行社交网络分析的技能
S0199	从数据包中提取和创造重要信息的技能
S0200	创造收集需求,以支持数据采集活动的技能。
S0201	创造计划以支持远程操作的技能
S0202	数据挖掘技术（例如，搜索文件系统）和分析的技能
S0203	定义和描述所有和操作环境相关的方面的技能
S0204	在网络地图上描述源或相关的数据的技能。
S0205	通过评估可用的功能来确定合适的目标选择，以达到预期的效果的技能
S0206	在各种操作系统上确定安装的补丁和识别补丁签名的技能。
S0207	在局域网和广域网环境中确定各种路由器和防火墙配置对业务模式和网络性能的影响的技能
S0208	确定网络设备的物理位置的技能
S0209	开发和执行全面的网络空间运营评估计划，以评估和验证业务性能和特征的技能。
S0210	发展情报报告的技能
S0211	开发或推荐分析方法或解决方案，以解决信息不完整或没有先例存在的问题和情况的技能。
S0212	及时传播项目的最高情报价值的技能。
S0213	记录和沟通复杂的技术和编程信息的技能。
S0214	对情报价值评估的技能
S0215	对元数据进行评估和解释的技能

S0216	评估可用的能力，提供有效的行动，以达到预期的效果的技能。
S0217	评估数据来源的相关性、可靠性和客观性的技能
S0218	评估信息的可靠性、有效性和相关性的技能
S0219	评估信息来识别相关性、优先级等技能。
S0220	开发/查询组织或合作伙伴收集的数据库的技能。
S0221	从数据包中提取信息的技能。
S0222	融合分析技能
S0223	生成操作计划,以支持任务和目标要求的技能
S0224	提高目标沟通能力
S0225	确定目标通信网络的技能
S0226	确定目标网络特征的技能
S0227	能够识别替代的解释分析方案，以尽量减少意外的结果的技能。
S0228	识别关键目标元素，包括网络域的关键目标元素的技能
S0229	识别可能危及组织/或合作伙伴利益的网络威胁的技能。
S0230	撤销，合并到 S0066
S0231	识别目标如何通信的技能
S0232	识别情报的不同和限制的技能。
S0233	识别可能对组织目标有影响的语言问题的技能
S0234	确定以开发为目标的线索的技能
S0235	识别非目标区域语言的技能
S0236	标识在每个级别的协议模型工作的设备的技能
S0237	通过地理空间分析技术识别、定位和跟踪目标的技能
S0238	涉及到操作的信息优化的技能
S0239	解释和编译编程语言的技能
S0240	作为采集系统的应用，解释元数据和内容的技能。
S0241	解释跟踪路由的结果,以适用于网络分析和重建的技能。
S0242	解释漏洞扫描器结果来识别漏洞的技能
S0243	知识管理的技能，包括技术文档（例如，wiki 页面）
S0244	管理客户关系,包括确定客户需求/需求,管理客户期望,和展示承诺提供高质量的结果的技能。
S0245	操纵网络可视化软件的技能
S0246	数目规范化的技能
S0247	从现有的情报进行数据融合，为了启用新的和继续性收集的技能。
S0248	对目标系统进行分析的技能
S0249	准备和展示简报的技能
S0250	准备计划及相关通信的技能
S0251	优先处理重要的目标语言的技能
S0252	处理收集到的数据为了方便后续分析的技能
S0253	提供与目标相关的分析的技能（例如，语言，文化，通信）。
S0254	提供分析，以帮助撰写阶段性行动报告的技能
S0255	利用目标基础设施提供实时的、可操作的地理定位信息的技能。
S0256	通过对物理、功能或行为关系的识别与分析，了解目标或威胁系统的技能。
S0257	阅读、翻译、写作、修改和执行简单的脚本（如 Perl、VBS）在 Windows 和 UNIX

	系统的技能（例如，那些执行解析大数据文件，自动手动任务，取/处理远程数据）
S0258	识别和解释在热点事件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	认识到中点的机会和必要的信息的技能。
S0261	认识信息的相关性的技能。
S0262	识别目标通信模式的重大变化的技能
S0263	识别用于元数据分析的技术信息的技能。
S0264	识别技术信息,可以用于导致启用远程操作的技能(数据包括用户、密码、电子邮件地址、IP 范围的目标,频率 DNI 行为、邮件服务器、域名服务器、SMTP 头信息)。
S0265	识别可用于目标开发的技术信息，包括情报开发的技能
S0266	了解相关的编程语言的技能（如 C++，Python 等）。
S0267	远程命令行和图形用户界面（GUI）工具使用的技能。
S0268	研究基本信息的技能
S0269	在热点安全事件中研究缺陷和漏洞利用的技能。
S0270	逆向工程（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的技能。
S0271	审查和编辑评估产品的技能
S0272	审查和编辑来自各种来源的情报产品用于网络操作的技能。
S0273	审查和编辑计划的技能
S0274	审查和编辑目标材料的技能
S0275	服务器管理的技能.
S0276	无线局域网元数据的调查、收集与分析的技能
S0277	综合分析，优先考虑数据集的意义的技能
S0278	必要层次的剪裁分析的技能（例如，分类和组织）
S0279	集合操作以直接支持目标开发的技能。
S0280	目标网络异常识别的技能（例如，入侵，数据流、新技术的目标实施等）
S0281	技术写作的技能
S0282	测试和评估工具的实现的技能
S0283	抄录目标语言通信的技能
S0284	翻译目标图形/或声音的语言材料的技能
S0285	使用布尔操作符构造简单和复杂的查询的技能
S0286	使用数据库识别目标相关信息的技能
S0287	利用地理空间数据和应用地理空间资源的技能
S0288	使用多个分析工具，数据库，和技术的技能（例如，分析师的笔记本、操作、Anchory、M3、发散/收敛思维、链接图表、矩阵等）。
S0289	使用多个搜索引擎（如谷歌，雅虎，LexisNexis, DataStar）和工具进行开源搜索的技能
S0290	使用 non-attributable 无主网络的技能
S0291	使用多个、不同来源的研究方法对目标网络进行重构的技能。
S0292	使用目标数据库和软件包的技能
S0293	使用工具、技术和程序对目标进行远程控制和建立持久性链接的技能
S0294	使用适用于网络分析和重建的跟踪路由工具，并解释其反馈结果的技能
S0295	使用各种开源的数据收集工具的技能（例如:网上贸易，DNS，邮件等）。

S0296	利用反馈，来改善流程，产品和服务的技能
S0297	使用虚拟的协同工作室或工具的技能（例如，IWS，VTCs，聊天室，SharePoint）。
S0298	验证所有文件的完整性的技能
S0299	对无线网络目标分析、模板和地理位置掌握的技能。
S0300	为缩小技术能力的差距，撰写（并提交）具体要求的技能。
S0301	以清晰、有说服力、有组织的方式书写事实和思想的技能
S0302	书写效果报告的技能。
S0303	撰写，审查和编辑网络相关的情报，并从多个来源评估产品的技能
S0304	访问当前可用资源的信息，及用法的技能。
S0305	访问需要维护计划/指令/指导的数据库的技能
S0306	分析并指导需要澄清或额外指导的问题的技能。
S0307	分析目标或威胁源的基本情况和想法的技能
S0308	根据就业需求预测情报能力的技能。
S0309	预见可能导致领导决策的关键目标或威胁活动的技能。
S0310	运用分析标准评估情报产品的技能
S0311	应用适用于组织目标的可用平台，传感器，架构和设备的功能，限制和任务方法的技能
S0312	通过应用过程来评估网络空间运营的性能和影响的技能。
S0313	阐明需求要求，并将新的和新兴的收集能力，访问或过程集成到收集操作中的技能。
S0314	拥有清晰的情报能力来支持计划的执行的技能
S0315	阐明联合计划者对所有来源分析师的需求的技能
S0316	将情报差距与优先信息的要求和可观察性结合起来的技能。
S0317	拥有比较和对比指标/量的要求的技能
S0318	概念化整个情报过程的多个域和维度的技能
S0319	拥有将情报需求转化为情报生产的职责技能。
S0320	协调定制情报产品的开发的技能
S0321	将情报优先级与情报资源/资产的分配相关联的技能
S0322	技术进展指标或成功的标准制定的技能
S0323	建立和维护最新的计划文件和跟踪服务/生产的技能。
S0324	判定信息采集的可行性的技能。
S0325	制定一个清楚地显示了各个岗位角色职能，可以用来收集所需的信息的收集计划的技能。
S0326	区分名义资源和实际资源及其对正在制定的计划的适用性的技能
S0327	确保充分利用所有可用资源来收集策略的技能
S0328	评估操作环境对目标和信息需求的影响因素的技能
S0329	评估信息来确定是否存在响应信息的请求的技能。
S0330	系统的评估剧院，国家，联盟和其他方面收集能力的能力，限制和任务方法的技能。
S0331	以口头和书面形式表达情报能力限制与决策风险之间的关系以及对整体运营的影响的技能。
S0332	从与收集要求和收集操作管理相关联的可用工具和应用中提取信息的技能。
S0333	图形描绘包含情报和合作伙伴能力估计的决策支持材料的技能。
S0334	确定和应用任务，收集，处理，利用和传播到相关的收集技术的技能
S0335	识别情报差距的技能。

S0336	识别何时满足优先级高的信息的要求的技能
S0337	执行评估收集管理和运营活动的程序的技能。
S0338	解释计划指导，以确定所需的分析支持水平的技能
S0339	解释准备报告，其运作的相关性和情报收集的影响的技能
S0340	监控目标或威胁的情况和环境因素的影响的影响
S0341	监视那些对合作伙伴能力有影响的威胁，并对其一直维护评估的技能
S0342	通过反复调整、测试和重新调整来优化收集系统的性能的技能。
S0343	协调情报计划小组，协调收集和生产情报支持，并监控状态的技能。
S0344	准备和提供报告，演示和简报，包括使用视觉辅助或演示技术的技能
S0345	将情报资源/资产与预期情报需求联系起来的技能
S0346	解决相互冲突的采集需求的技能。
S0347	审查收集到的资产的性能规格和历史信息的技能。
S0348	指定必须在短期内进行的集合或任务的技能
S0349	与关键信息需求过程同步的操作评估程序的技能。
S0350	同步规划活动和所需的情报支持的技能
S0351	系统的翻译剧院，国家，联盟和其他方面收集能力的能力，限制和任务方法的技能。
S0352	使用协作工具和环境的技能。
S0353	使用系统或工具跟踪搜集需求，并确定它们是否满足要求的技能。
S0354	创建反映业务核心隐私目标的政策的技能
S0355	与供应商谈判协议和评估供应商隐私的做法的技能。
S0356	与各级管理人员包括董事会成员的沟通的技能（例如，人际交往能力、亲和力、有效的倾听技巧，为观众恰当地使用风格和语言）。
S0357	预见新的安全威胁的技能。
S0358	意识到不断发展的技术基础设施的技能。
S0359	运用批判性思维分析组织模式和关系的技能。

A.7 NCWF 能力描述

表 8 提供了网络空间安全岗位从业人员需要具备的专业能力列表。这个列表中罗列的能力也被收录在附录 B 岗位角色的详细描述中。由于这些技能已经久经演化，并且将继续演化下去，所以并没有以特定的标准排序，而将以简单的方式按序号添加。

表格 8 NCWF 能力描述

ID	描述
A0001	基于漏洞和配置数据的分析识别系统安全问题的能力
A0002	为给定的应用或环境匹配合适的知识库技术的能力
A0003	能够确定技术趋势数据有效性的能力
A0004	能够开发课程，针对目标用户在合适的水平上进行讲解
A0005	解密数字数据集合的能力
A0006	准备和提供（安全）培训和意识教育素材的能力，确保系统、网络和数据的用户建立意识，并遵守系统安全策略和流程。

A0007	为应用特定关注点进行定制代码分析的能力
A0008	应用方法、标准来描述、分析和文档化组织机构的企业 IT 架构（比如 TOGAF、DODAF、FEAF）
A0009	应用供应链风险管理标准的能力
A0010	分析恶意软件的能力
A0011	清晰简洁的方式回答问题的能力
A0012	清晰提问题的能力
A0013	通过口头的、书面的、视觉的方式，通过友好的、精心组织的方法，传递复杂信息、概念或想法的能力
A0014	通过写作有效沟通的能力
A0015	在安全系统中进行漏洞扫描并识别漏洞的能力
A0016	促进小组讨论的能力
A0017	评估学习者理解力和知识水平的能力
A0018	准备和呈现简报的能力
A0019	编写技术文档的能力
A0020	为学生提供有效反馈来提高学习效果的能力
A0021	使用和理解复杂数学概念的能力（比如离散数学）
A0022	应用成人学习原则的能力
A0023	设计有效的、可靠的评估方法的能力
A0024	开发方向清晰并有指导性的教学素材的能力
A0025	在故障工单系统中精确定义事件、问题和事件的能力
A0026	分析测试设计的能力
A0027	应用组织机构的目标来开发和维护架构的能力
A0028	评估和预测人力需求，满足组织机构目标要求的能力
A0029	能够建立复杂数据结构和高层次编程语言的能力
A0030	收集、检验和验证测试数据的能力
A0031	能力进行市场研究，弄清政府和行业能力，合适定价。
A0032	在虚拟机环境里设计开发可用（网安）课程的能力
A0033	能够制定符合法律、规定、政策和标准要求的策略、规划和战略，来支持组组织机构的网络空间行动。
A0034	能够开发、更新和/或维护标准操作程序（SOP）
A0035	能够对问题进行研究并检查那些看起来可能无关数据之间的联系。
A0036	能够在更高水平看出基本的常见编码缺陷
A0037	能够充分用最佳实践和从外部组织机构和研究机构学来的课程，来处理网络空间问题。
A0038	能够对系统进行优化，满足企业性能需求。
A0039	能够对成本估算生命周期的变化和更新进行监管。
A0040	能够将数据和测试结果转为可评估的结论。
A0041	能够使用数据可视化工具（比如 Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js）
A0042	能够创造职业发展机会
A0043	能够在 Windows 和 Nnix/Linux 环境下进行取证分析
A0044	能够使用编程语言结构（比如代码审查）和逻辑

A0045	能够评估/确认供应商和/或产品的可信性。
A0046	能够监控和评估新兴技术对法律、规定和/或政策的潜在影响
A0047	能够根据安全软件开发方法论、工具和实践来开发安全软件。
A0048	能够应用网络安全架构概念，包括拓扑、协议、组件和原则（比如应用纵深防御）
A0049	能够应用安全系统设计工具、方法和技术
A0050	能够应用包括自动化系统分析和设计工具在内的系统设计工具、方法和技术。
A0051	能够执行技术集成的流程
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	能够判断（网安）人才趋势数据的有效性
A0054	能够应用教学系统设计（ISD）方法论
A0055	能够操作常见的网络工具（比如 ping、tracerout、nslookup）
A0056	确保收购过程中遵循安全措施的能力。
A0057	能够根据目标用户的水平，针对性的裁剪培训课程。
A0058	能够执行操作系统命令行命令（比如 ipconfig\netstat\dir\nbtstat）
A0059	能够操作组织机构的 LAN/WAN 网络路径
A0060	能够构建架构和框架
A0061	能够设计架构和框架
A0062	能够监控系统性能和可用性的指标
A0063	能够操作不同的电子通信系统和方法（比如电子邮件、VOIP、即时通讯、Web 论坛、直接视频广播）
A0064	能够将客户需求转化为运营能力
A0065	能够监控网络流量
A0066	能够精准的、完整的将情报、评估和/或规划产品中使用的所有数据确定来源。
A0067	能够在一个多样的、无法预期的、充满挑战的以及快节奏的工作环境中应用并工作。
A0068	能够将经过批准的规划落地，执行员工配置流程
A0069	能够应用协作的技能和策略。
A0070	具备进行批判式阅读和思考的技能
A0071	能够利用语言和文化特长进行分析
A0072	能够清晰的将情报需求表述为良好的研究课题和可跟踪的数据变量，从而进行探究和跟踪。
A0073	能够清晰的将情报需求表述为良好的研究课题和信息需求。
A0074	能够与他人有效合作
A0075	能够通过口头、书面和/或视频的形式，以自信、组织良好的方式沟通复杂信息、概念或想法。
A0076	能够在监控需求和关键信息开发上，与分析师协调合作
A0077	能够与其他机构的职责或支持活动协调网络空间行动。
A0078	能够与下级、平级和上级机构协调、合作和传播信息。
A0079	能够正确的将每个机构或元素放到（信息）收集计划和矩阵中
A0080	在面对问题和信息不完整或者没有先例存在的情况下，能够给出分析方法或解决方案建议，

A0081	在面对问题和没有先例存在的情况下，能够给出计划方案或建议。
A0082	能够通过虚拟团队进行有效合作
A0083	能够评估信息的可靠性、有效性和相关性。
A0084	能够评估、分析和综合大量数据（可能是支离破碎和互相矛盾的），形成高质量的、多方面融合的靶标/情报产品。
A0085	在政策不明确时，能够进行（合适）判断。
A0086	为了识别感兴趣的目标，能够进行目标分析和（信息收集）扩大网络访问
A0087	能够专注研究工作，满足客户的决策需求。
A0088	能够在动态的、快节奏的环境中有效工作。
A0089	能在一个协作环境中工作，与机构内部的和外部其他分析师和专家寻求持续的协商，实现分析能力和技术能力的共赢
A0090	能够识别有共同网络空间行动兴趣的外部合作伙伴
A0091	能够识别情报漏洞
A0092	能够识别/描述目标漏洞
A0093	能够进行靶标技术利用时，识别（或描述）技术（或方法）。
A0094	能够解释和应用与机构网络空间目标相关的法律、规定、政策和指南。
A0095	能够将客户需求转化为可操作的行动
A0096	能够解释和理解，复杂的、快速变化的概念
A0097	能够监控系统运营，并对触发事件和/或观察到的趋势或异常活动进行响应。
A0098	必要时可以作为规划组成员、协助组成员和工作组成员参与（工作）
A0099	能够执行网络收集策略、技术和包括解密能力/工具在内的程序。
A0100	能够执行包括解密能力/工具在内的无线收集程序。
A0101	能够认识和减轻可能影响分析效果的认知偏见。
A0102	能够认识和减轻报告和分析中的欺骗（内容）
A0103	能够审查经过处理的目标语言材料的准确性和完整性
A0104	能够选择合适植入（程序）来达到操作目标。
A0105	能够根据客户理解水平定制技术和计划信息
A0106	具有批判性思维
A0107	能够像威胁攻击者一样思考
A0108	能够理解目标和效果
A0109	能够在所有情报科目中使用多个情报来源
A0110	能够关注信息隐私法律的发展，确保组织机构能够适应并符合其要求
A0111	能够跨部门和业务单元工作，实现组织机构隐私原则和程序，并且将隐私目标与（组织机构）安全目标相对照协调。
A0112	能够关注信息隐私技术的发展，确保组织机构能够适应并符合要求
A0113	能够确定一个安全事件是否违反了隐私原则或法律要求，需要采取法律行动。
A0114	能够开发或采购课程，为目标（用户）提供合适的培训主题。
A0115	能够跨部门和业务单元工作，实现组织机构隐私原则和程序，并且将隐私目标与（组织机构）安全目标相对照协调。 （与 A0111 完全重合）
A0116	能够正确有效的对网络空间安全资源设置优先级并分配。
A0117	能够在组织机构动态环境中将战略、业务和技术联系起来。
A0118	能够理解组织机构流程和问题解决相关的技术、管理和领导力话题。

A0119	能够理解网络空间和它的组织影响相关的基本概念和话题。

附录 B—岗位角色详细列表

以下部分提供了 NCWF 每一个岗位角色的详细描述。下面的列表为 NCWF 的每一个岗位角色提供了以下信息：

- 唯一的 NCWF 岗位角色 ID，这个 ID 根据岗位角色所属的 NCWF 类别和专业领域编制。
- 岗位角色匹配的专业领域
- 岗位角色的正式名称，后面紧接的圆括号中是 OPM job 代码识别号
- 岗位角色的描述
- 位于该岗位角色的网络空间安全从业人员，被期望履行的 NCWF 职责清单
- 位于该岗位角色的网络空间安全从业人员，被期望展示的 NCWF 知识点清单
- 位于该岗位角色的网络空间安全从业人员，被期望掌握的 NCWF 技能清单
- 位于该岗位角色的网络空间安全从业人员，被期望展现的 NCWF 能力清单

以下表格描述了 NCWF 岗位角色。如在第四部分所述，这个列表将根据业界反馈和网络空间安全前景的变化定期更新。

岗位角色 ID	**SP-RM-001**
类别	安全基础设施提供（SP）
专业领域	风险管控（RM）
岗位角色名字	授权官员/指定代表
岗位角色描述	获得授权的高级官员或主管将正式承担责任，在对组织机构运营、组织机构资产、个人、其他组织机构和国家而言的合理风险范围内，进行信息系统的运营工作（CNSSI 4009).
岗位职责	T0145, T0221, T0371, T0495
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0084, K0085, K0089, K0101, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342
技能	S0034
能力	[未指定]

岗位角色 ID	**SP-RM-002**
类别	安全基础设施提供（SP)
专业领域	风险管控（RM）
岗位角色名字	安全控制评估师(612)
岗位角色描述	对管理、运营、技术安全控制和内置的或从某个 IT 系统继承的控制增强装置，进行独立的、综合的评估，以确定安全控制的整体有效性。
岗位职责	T0032, T0072, T0079, T0083, T0141, T0150, T0183, T0184, T0197, T0218, T0221, T0244, T0245, T0251, T0301

知识	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0084, K0085, K0089, K0101, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342
技能	S0001, S0006, S0027, S0034, S0038, S0086
能力	[未指定]

岗位角色 ID	**SP-DEV-001**
类别	安全基础设施提供 (SP)
专业领域	软件开发 (DEV)
岗位角色名字	软件开发者 (621)
岗位角色描述	开发、创建、维护、编写/编码 新的（或修改现有的）计算机应用、软件或专门的实用程序。
岗位职责	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, K0051, K0060, K0066, K0068, K0073, K0079, K0080, K0081, K0082, K0084, K0085, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0219, K0260, K0261, K0262, K0263, K0322, K0331, K0342, K0343
技能	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175
能力	A0007, A0021, A0047

岗位角色 ID	**SP-DEV-002**
类别	安全基础设施提供 (SP)
专业领域	软件开发 (DEV)
岗位角色名字	安全软件评估师 (622)
岗位角色描述	对新的或现有的计算机应用、软件或专门的实用程序进行安全分析并提供可操作的结果。
岗位职责	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, K0051, K0060, K0066, K0068, K0073, K0079, K0080, K0081, K0082, K0084, K0085, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0219, K0260, K0261, K0262, K0263, K0322, K0342, K0343
技能	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175

能力	A0021

岗位角色 ID	SP-ARC-001
类别	安全基础设施提供（SP）
专业领域	系统架构（ARC）
岗位角色名字	企业架构师(651)
岗位角色描述	开发并维护业务、系统和信息处理过程，支持企业使命目标。开发符合基准和目标架构的信息技术规则和需求。
岗位职责	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
技能	S0005, S0024, S0050, S0060, S0099, S0122
能力	A0008, A0015, A0027, A0038, A0051, A0060

岗位角色 ID	SP-ARC-002
类别	安全基础设施提供（SP）
专业领域	系统架构(ARC)
岗位角色名字	安全架构师(652)
岗位角色描述	规划企业和系统安全，贯穿整个开发生命周期，将技术和环境条件（比如法律和法规）融入到安全的设计与过程中。
岗位职责	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, K0015, K0018, K0019, K0024, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0060, K0061, K0063, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0207, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0332, K0333, K0336
技能	S0005, S0024, S0027, S0050, S0060, S0099, S0116, S0122, S0139, S0152, S0168
能力	A0008, A0015, A0027, A0038, A0048, A0049, A0050, A0061

岗位角色 ID	SP-RD-001

类别	安全基础设施提供 (SP)
专业领域	技术研发 (RD)
岗位角色名字	研发专家 (661)
岗位角色描述	研究软件系统，以开发新功能，确保与网络空间安全完全集成。进行综合广泛的技术研究来评估网络空间系统中的潜在漏洞。
岗位职责	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0169, K0170, K0171, K0172, K0173, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342
技能	S0005, S0017, S0072, S0140, S0148, S0172
能力	A0001, A0018, A0019

岗位角色 ID	**SP-RP-001**
类别	安全基础设施提供 (SP)
专业领域	系统需求规划 (RP)
岗位角色名字	系统需求规划师 (641)
岗位角色描述	与客户协商评估功能需求，并将功能需求转化为技术解决方案。
岗位职责	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, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333
技能	S0005, S0006, S0008, S0010, S0050, S0134
能力	A0064

岗位角色 ID	**SP-TE-001**
类别	安全基础设施提供 (SP)
专业领域	测试评估 (TE)
岗位角色名字	系统测试和评估专家(671)
岗位角色描述	计划、准备和执行系统测试，对照（系统）规格和需求评估测试结果，分析/汇报测试结果。
岗位职责	T0058, T0080, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0102, K0139, 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
能力	A0026, A0030, A0040

岗位角色 ID	SP-SYS-001
类别	安全基础设施提供 (SP)
专业领域	系统开发 (SYS)
岗位角色名字	信息系统安全开发者(631)
岗位角色描述	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的安全性。
岗位职责	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, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0331, K0333, K0336
技能	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160
能力	[未指定]

岗位角色 ID	SP-SYS-002
类别	安全基础设施提供 (SP)
专业领域	系统开发 (SYS)
岗位角色名字	系统开发者 (632)
岗位角色描述	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。
岗位职责	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, 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, S0031, S0034, S0036, S0060, S0085, S0097, S0098, S0136, S0145, S0146, S0160
能力	[未指定]

岗位角色 ID	OM-DA-001
类别	运营与维护 (OM)
专业领域	数据管理 (DA)
岗位角色名字	数据库管理员 (421)
岗位角色描述	管理用于存储、查询和调用数据的数据库和/或数据管理系统。
岗位职责	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, K0260, K0261, K0262, K0277, K0278, K0279, K0287, K0420
技能	S0002, S0013, S0037, S0042, S0045
能力	[未指定]

岗位角色 ID	OM-DA-002
类别	运营与维护 (OM)
专业领域	数据管理 (DA)
岗位角色名字	数据分析 (422)
岗位角色描述	对多个不同来源的数据进行检查分析，以发现新的洞见。针对用于数据建模、数据挖掘以及数据研究的复杂的、企业级规模的数据集，设计并实现自定义算法、流程和布局。
岗位职责	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, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0328, K0420
技能	S0013, S0017, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0105, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160
能力	A0029, A0035, A0036, A0041, A0066

岗位角色 ID	OM-KM-001
类别	运营与维护 (OM)

专业领域	知识管理(KM)
岗位角色名字	知识管理管理者(431)
岗位角色描述	负责管理和运营（知识管理）的流程和工具。这些过程和工具可以让组织机构可以识别、记录和访问智力资本和信息内容。
岗位职责	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

岗位角色 ID	**OM-TS-001**
类别	运营与维护 (OM)
专业领域	客户服务和技术支持 (TS)
岗位角色名字	技术支持专家 (411)
岗位角色描述	利用客户级的硬件和软件，对需要帮助的客户提供技术支持，严格遵循已有的或已批准的组织机构流程组件（如主机事件管理计划，如适用时）。
岗位职责	T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0114, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0306, K0317, K0330
技能	S0039, S0058, S0142, S0159
能力	A0025, A0034

岗位角色 ID	**OM-NET-001**
类别	运营与维护 (OM)
专业领域	网络服务 (NET)
岗位角色名字	网络运营专家(441)
岗位角色描述	对包括硬件和虚拟环境在内的网络服务/系统，进行计划、实施和运营。
岗位职责	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, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0181, K0200, K0201, K0203, K0260, K0261, K0262, K0287, K0307, K0332
技能	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
能力	A0052, A0055, A0058, A0059, A0062, A0063, A0065

岗位角色 ID	OM-SA-001
类别	运营与维护 (OM)
专业领域	系统管理 (SA)
岗位角色名字	系统管理员 (451)
岗位角色描述	对硬件和软件进行安装、配置、故障解决和维护，管理系统账号。
岗位职责	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, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0181, K0260, K0261, K0262, K0280, K0289, K0318, K0327, K0331, K0346
技能	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
能力	[未指定]

岗位角色 ID	OM-AN-001
类别	运营与维护 (OM)
专业领域	系统分析(AN)
岗位角色名字	系统安全分析师(461)
岗位角色描述	负责对系统安全集成、测试、运行和维护进行分析和开发。
岗位职责	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, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0232, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0329, K0333, K0339
技能	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167
能力	A0015

岗位角色 ID	OV-LG-001
类别	监管与治理 (OV)
专业领域	法律咨询和辩护 (LG)
岗位角色名字	网络空间法律顾问 (731)
岗位角色描述	对网络空间相关法律话题，提供专业的法律意见和建议。
岗位职责	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, K0312, K0316, K0341
技能	[未指定]

能力	A0046

岗位角色 ID	OV-LG-002
类别	监管与治理 (OV)
专业领域	法律咨询和辩护 (LG)
岗位角色名字	隐私合规管理者 (732)
岗位角色描述	督促、监管隐私合规项目以及隐私项目工作人员，帮助安全工作人员和他们团队的满足隐私合规要求。
岗位职责	T0003, T0004, 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, K0606, K0607, K0608, K0609, K0610, K0611, K0612, K0613, K0614
技能	S0354, S0355, S0356
能力	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115

岗位角色 ID	OV-ED-001
类别	监管与治理 (OV)
专业领域	培训、教育和养成 (ED)
岗位角色名字	网络空间教程开发者 (711)
岗位角色描述	根据教学计划需求，开发、规划、协调和评估网络空间培训/教育课程、方法和技术。
岗位职责	T0230, T0247, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0534, T0536, T0926
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0239, K0245, K0246, K0252, K0287
技能	S0064, S0066, S0070, S0102, S0166
能力	A0004, A0032, A0054

岗位角色 ID	OV-ED-002
类别	监管与治理 (OV)
专业领域	培训、教育和养成 (ED)
岗位角色名字	网络空间讲师 (712)
岗位角色描述	制定和实施网络空间领域从业人员的培训或教学。
岗位职责	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0443, T0444, T0450, T0467,

	T0519, T0520, T0535, T0536, T0926
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0287, K0319
技能	S0064, S0070, S0100, S0101
能力	A0006, A0011, A0012, A0013, A0014, A0016, A0017, A0020, A0022, A0023, A0024, A0057

岗位角色 ID	**OV-MG-001**
类别	监管与治理 (OV)
专业领域	网络空间安全管理(MG)
岗位角色名字	信息系统安全管理者 (722)
岗位角色描述	负责一个程序、组织机构、系统或飞地的网络空间安全。
岗位职责	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
技能	S0018, S0027, S0086
能力	[未指定]

岗位角色 ID	**OV-MG-002**
类别	监管与治理 (OV)
专业领域	网络空间安全管理(MG)
岗位角色名字	通信安全管理者(723)
岗位角色描述	管理一个组织机构的通信安全资源（CNSSI 4009）
岗位职责	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, K0287
技能	S0027
能力	[未指定]

岗位角色 ID	OV-PL-001
类别	监管与治理 (OV)
专业领域	战略规划和策略 (PL)
岗位角色名字	网络空间人力开发者和管理者 (751)
岗位角色描述	制定网络空间人才规划、战略和指南，以支持网络空间人才的人力、人才、培训和教育需求，应网络空间政策、条款、材料、人员结构、以及教育和培训需求而变化。
岗位职责	T0074, T0094, T0116, T0222, T0226, T0341, T0355, T0356, T0362, T0363, T0364, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0537, T0552
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0166, K0168, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
技能	S0108, S0128
能力	A0028, A0033, A0037, A0042, A0053

岗位角色 ID	OV-PL-002
类别	监管与治理 (OV)
专业领域	战略规划和策略（PL）
岗位角色名字	网络空间策略和战略规划师 (752)
岗位角色描述	制定网络空间规划、战略和政策，与组织机构网络空间的使命和宗旨相符。
岗位职责	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
技能	[未指定]
能力	A0003, A0033, A0037

岗位角色 ID	OV-EX-001
类别	监管与治理 (OV)
专业领域	网络空间安全执行领导 (EX)
岗位角色名字	网络空间安全执行领导 (901)
岗位角色描述	制定权威决策，建立组织机构网络空间和网络空间相关资源和/或业务的愿景和方向。
岗位职责	T0001, T0002, T0006, T0066, T0157, T0229, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0085, K0106, K0314, K0296, K0147
技能	S0356, S0357, S0358, S0359
能力	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117,

	A0118, A0119

岗位角色 ID	OV-PM-001
类别	监管与治理 (OV)
专业领域	采购和项目管理(PM)
岗位角色名字	项目管理者 (801)
岗位角色描述	领导、协调、沟通、整合，并对项目的全面成功负责，确保符合关键代理优先级。
岗位职责	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, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
技能	S0038
能力	A0009, A0039, A0045, A0056,

岗位角色 ID	OV-PM-002
类别	监管与治理 (OV)
专业领域	采购和项目管理(PM)
岗位角色名字	IT 项目管理者 (802)
岗位角色描述	直接管理 IT 项目，提供独特的服务或者产品。
岗位职责	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, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
技能	S0038
能力	A0009, A0039, A0045, A0056

岗位角色 ID	OV-PM-003
类别	监管与治理 (OV)
专业领域	采购和项目管理 (PM)
岗位角色名字	产品支持管理者 (803)
岗位角色描述	管理现场支持所需的功能包，保持系统和组件的就绪状态和业务能力。
岗位职责	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, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
技能	S0038
能力	A0009, A0031, A0039, A0045, A0056

岗位角色 ID	OV-PM-004
类别	监管与治理 (OV)
专业领域	采购和项目管理 (PM)
岗位角色名字	IT 投资和投资组合管理者 (804)
岗位角色描述	掌管 IT 能力的投资组合，使其符合企业使命的总体要求和组织机构优先事项。
岗位职责	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	[未指定]
能力	A0039

岗位角色 ID	OV-PM-005
类别	监管与治理 (OV)
专业领域	采购和项目管理(PM)
岗位角色名字	IT 项目审计(805)
岗位角色描述	对 IT 项目或它的单独组件进行评估，确保它们符合已发布的标准。
岗位职责	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
技能	S0038, S0085
能力	A0056

岗位角色 ID	PR-DA-001
类别	保护和防御 (PR)
专业领域	网络空间安全防御分析(DA)
岗位角色名字	网络空间安全防御分析师 (511)
岗位角色描述	使用从自多个网络防御工具（比如 IDS 告警、防火墙、网络流量日志）收集而来的数据，研究分析这些环境中发生的事件，从而抑制安全威胁。
岗位职责	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, K0099, K0104, K0106, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0273, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0331, K0339, K0342
技能	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0167, S0169
能力	A0010, A0015, A0066

岗位角色 ID	**PR-INF-001**
类别	保护和防御 (PR)
专业领域	网络空间安全防御基础设施支持 (INF)
岗位角色名字	网络空间安全防御基础设施支持专家 (521)
岗位角色描述	测试、实施、部署、维护和管理硬件和软件基础设施。
岗位职责	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0331, K0334, K0340
技能	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124
能力	[未指定]

岗位角色 ID	**PR-IR-001**
类别	保护和防御 (PR)
专业领域	事件响应 (IR)
岗位角色名字	网络空间防御事件响应员(531)
岗位角色描述	针对网络环境或飞地内的网络事件进行调查、分析和响应。
岗位职责	T0041, T0047, T0161, T0163, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0333, 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, K0225, K0230, K0259, K0287, K0332
技能	S0003, S0047, S0077, S0078, S0079, S0080, S0173
能力	[未指定]

岗位角色 ID	**PR-VA-001**
类别	保护和防御 (PR)
专业领域	漏洞评估和管理 (VA)
岗位角色名字	漏洞评估分析师(541)
岗位角色描述	在网络环境或飞地中对系统和网络进行评估，找出哪些系统 / 网络

	偏离了合理配置、飞地政策或本地政策。评测应对已知漏洞的纵深防御架构的有效性。
岗位职责	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, K0085, K0089, K0106, K0139, K0161, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0331, K0342, K0344, K0345
技能	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171
能力	A0001, A0044

岗位角色 ID	**AN-TA-001**
类别	分析(AN)
专业领域	威胁分析 (TA)
岗位角色名字	预警分析师 (141)
岗位角色描述	开发独特的网络空间指标，以保持在高动态运行环境下对（系统）运行状态的持续感知。收集、处理、分析并传达网络告警评估（信息）。
岗位职责	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, K0173, K0348, K0349, K0362, K0369, K0370, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, 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	A0066, A0072, A0075, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

岗位角色 ID	**AN-XA-001**
类别	分析(AN)
专业领域	渗透分析(XA)
岗位角色名字	渗透分析师 (121)
岗位角色描述	通过协作，找出获取信息和搜集信息的空白区，通过网络采集和/或准备活动来填补空白。利用所有授权资源和分析技术渗透目标网络。
岗位职责	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, K0131, K0142,

	K0348, K0349, K0362, K0369, K0370, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0434, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0537, 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	A0066, A0075, A0080, A0084, A0074, A0086, A0092, A0093, A0104

岗位角色 ID	**AN-AN-001**
类别	分析(AN)
专业领域	全源分析 (AN)
岗位角色名字	全源分析师 (111)
岗位角色描述	分析来自一个或多个来源的数据/信息，创建准备环境，响应信息请求，并提交情报收集和生产要求，支持规划和运营。
岗位职责	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, K0348, K0349, K0362, K0369, K0370, 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, K0515, 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
能力	A0066, A0075, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

岗位角色 ID	**AN-AN-002**
类别	分析(AN)
专业领域	全源分析 (AN)
岗位角色名字	任务评估专家(112)
岗位角色描述	制定绩效考核计划和措施。对网络活动进行必要的战略层面和运营层面的效果评估。确定系统是否按照预期运行，为运行效能的测定提供建议。
岗位职责	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, K0348, K0349, K0362, K0369, K0370, 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
能力	A0066, A0075, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108

岗位角色 ID	**AN-TD-001**
类别	分析(AN)
专业领域	目标分析 (TD)
岗位角色名字	目标开发人员 (131)
岗位角色描述	执行目标系统分析，构建和/或维护电子目标文件夹，该文件夹包括了从环境准备、和/或内部或外部情报来源的所有情况。协调合作伙伴的目标活动和情报机构，提出备选目标进行审查和验证。
岗位职责	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, K0142, K0173, K0348, K0349, K0362, K0369, K0370, 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, 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
能力	A0066, A0075, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073
岗位角色 ID	**AN-TD-002**
类别	分析(AN)

专业领域	目标分析 (TD)
岗位角色名字	目标网络分析师 (131)
岗位角色描述	对收集的和开源的数据进行高级分析，确保目标连续性，为目标及其活动进行画像，开发技术以获取更多的目标信息。基于对目标技术、数字网络和网络上的应用程序的了解，确定目标是如何进行通信、移动、操作和生存的。
岗位职责	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, K0348, K0349, K0362, K0369, K0370, 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, 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	A0066, A0075, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

岗位角色 ID	**AN-LA-001**
类别	分析(AN)
专业领域	语言分析 (LA)
岗位角色名字	多学科语言分析师 (151)
岗位角色描述	运用目标/威胁相关的语言和文化专业知识和技术知识来处理，分析和/或传达来自语言，语音和/或图像材料的情报信息。创建和维护特定语言的数据库和工作辅助工具，以支持网络行动的执行，并确保关键知识的共享。在外语密集型或跨学科型项目中，提供相关的专业知识。
岗位职责	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, TO860
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0173, K0348, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0434, K0356, K0359, K0367, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, 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	A0075, A0089, A0071, A0103

岗位角色 ID	**CO-CL-001**
类别	搜集与运作 (CO)
专业领域	搜集与运作 (CL)
岗位角色名字	全源搜集管理者(311)
岗位角色描述	确定搜集机构和环境；将优先信息需求纳入收集管理；开发（相关）概念以支撑领导意图。确定可用的搜集资产能力，标识新的搜集功能，并构建和传播搜集计划。监控已委派的搜集任务的执行，确保搜集计划的高效执行。
岗位职责	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, K0431, K0449, K0417, K0579, K0596, K0369, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0366, 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
能力	A0069, A0070, A0076, A0078, A0079
岗位角色 ID	**CO-CL-002**
类别	搜集与运作 (CO)
专业领域	搜集与运作 (CL)
岗位角色名字	全源搜集需求管理者 (312)
岗位角色描述	使用现有的资源和方法，评估搜集运行情况，开发基于效果的搜集需求策略，提高搜集（效果）。开发、处理、验证和协调搜集需求的提交。评估搜集资产和搜集运营的表现。

岗位职责	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, K0431, K0417, K0579, K0596, K0369, K0444, K0395, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0353, K0361, K0364, K0366, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0421, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0521, K0526, K0527, K0552, K0554, K0558, K0562, K0563, K0568, K0569, K0570, K0580, K0581, K0584, K0587, K0588, K0605
技能	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353
能力	A0069, A0070, A0078

岗位角色 ID	**CO-PL-001**
类别	搜集与运作 (CO)
专业领域	网络空间运营规划 (PL)
岗位角色名字	网络空间情报规划师(331)
岗位角色描述	制定详细的情报计划，以满足网络空间运营需求。协助网络空间运营规划师，识别、验证和征集搜集与分析的需求。参与网络行动的目标选择、验证、同步和执行。同步情报活动，以支持组织机构在网络空间的目标。
岗位职责	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, K0173, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0348, K0377, K0349, K0362, K0370, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0374, K0378, K0399, K0400, K0408, K0411, K0422, K0432, K0441, K0455, K0456, K0459, K0463, K0494, 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, 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
能力	A0066, A0070, A0075, A0089, A0085, A0082, A0074. A0067. A0068. A0077. A0081. A0090. A0094. A0096. A0098. A0105

岗位角色 ID	**CO-PL-002**
类别	搜集与运作 (CO)
专业领域	网络空间运营规划(PL)
岗位角色名字	网络空间运营规划师 (332)
岗位角色描述	通过与其他规划师，运营人员和/或分析师协作，制定详细的计划，以引导或提示网络空间运营的合适范围。参与目标选择，验证，同步，并且在网络行动执行过程中实现集成。
岗位职责	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, K0173, K0431, K0417, K0444, K0395, K0445, K0560, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0348, K0377, K0349, K0362, K0370, K0436, K0379, K0403, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0347, K0350, K0352, K0374, K0378, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0494, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0518, K0519, K0525, K0538, K0566, K0572, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0516, K0497, K0534, K0576, K0597
技能	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349
能力	A0066, A0070, A0075, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

岗位角色 ID	**CO-PL-003**
类别	搜集与运作 (CO)
专业领域	网络空间运营规划 (PL)
岗位角色名字	合作伙伴集成规划师 (333)
岗位角色描述	推进跨组织或跨国界的网络合作伙伴之间的合作。通过提供指导，资源和协作，支援合作伙伴网络团队的整合，发挥最佳实践并促进组织机构在联动的网络行动中实现目标。

岗位职责	T0581, 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, T0762, T0766, T0817, T0818, T0825, T0826
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0173, K0431, K0417, K0444, K0395, K0435, K0392, K0348, K0377, K0362, K0370, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0374, K0400, K0408, K0411, K0422, K0432, K0455, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585
技能	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326
能力	A0066, A0070, A0075, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

岗位角色 ID	**CO-OP-001**
类别	搜集与运作 (CO)
专业领域	网络空间运营 (OP)
岗位角色名字	网络空间运营专员(321)
岗位角色描述	进行搜集、处理和/或地理定位，来渗透、定位和/或跟踪感兴趣的目标。进行网络导航、战术取证分析，并依据指示，执行线上操作。
岗位职责	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, K0142, K0370, K0379, K0403, K0560, K0565, K0480, K0516, K0427, K0440, K0430, K0537, K0608, K0360, K0363, K0365, K0372, K0373, K0375, K0406, K0420, K0423, K0428, K0429, K0433, K0438, K0452, K0468, K0481, K0485, K0486, K0528, K0530, K0531, K0536, K0573, 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
能力	A0095, A0097, A0099, A0100

岗位角色 ID	**IN-CI-001**
类别	调查 (IN)
专业领域	网络调查（CI）
岗位角色名字	网络空间犯罪调查专员 (221)
岗位角色描述	采用可控的、有据可依的分析调查技术，对证据进行识别、收集、检

	查和保存。
岗位职责	说明：其中几项活动只能由执法人员或反情报管理局人员进行。 T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0114, K0118, K0123, K0128, K0144, K0168, K0231, K0244, K0251
技能	S0047, S0068, S0072, S0086, S0165
能力	[未指定]

岗位角色 ID	**IN-FO-001**
类别	调查(IN)
专业领域	数字取证 (FO)
岗位角色名字	取证分析师(211)
岗位角色描述	对基于计算机的犯罪进行深度调查，包括与网络入侵事件相关的数字介质和日志。 针对基于计算机的犯罪进行深度调查，建立文档证据或物证，包括与网络入侵事件相关的数媒文件和日志。
岗位职责	T0067, T0076, T0096, T0115, T0146, T0484, T0220, T0235, T0273, T0297, T0398, T0401, T0403, T0411, T0425, T0421, T0424, T0440, T0482, T0490, T0507, T0274, T0059, T0541, T0558, T0078, T0427, T0402, T0419, T0420, T0542, T0308, T0447
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0099, 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
技能	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
能力	A0005

岗位角色 ID	**IN-FO-002**
类别	调查(IN)
专业领域	数字取证 (FO)
岗位角色名字	网络空间防御取证分析师 (212)
岗位角色描述	分析数字证据，调查计算机安全事件，以获取有用的信息，消除系统/网络安全隐患。
岗位职责	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165,

	T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0543, T0546
知识	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0099, 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
技能	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133
能力	A0005, A0043

附录 C—缩写词

本文中用到的缩写词说明如下：

API Application programming interface/应用编程接口

CAE Centers of Academic Excellence/卓越学术中心

CDS Cross-Domain Solutions/跨域解决方案

CIO Chief Information Officer/首席信息官

CMMI Capability Maturity Model Integration/能力成熟度模型集成

CNSSI Committee on National Security Systems Instruction/国家安全系统指令委员会

COMSEC Communications Security/通信安全

COTR Contracting Officer's Technical Representative/合同事务处技术代表

CSF Cybersecurity Framework/网络空间安全框架

CSIP Cybersecurity Strategy and Implementation Plan/网络空间安全战略和实施计划

DNS Domain Name System/域名系统

EISA Enterprise information security architecture/企业信息安全架构

FISMA Federal Information Security Modernization Act/联邦信息安全现代化法案

FOIA Freedom of Information Act/信息自由法案

HR Human Resource/人力资源

IDS Intrusion detection system/入侵检测系统

IP Internet Protocol/IP 协议

IPS Intrusion Prevention System/入侵防御系统

IR Incident Response/事件响应

IRT Incident Response Teams/事件响应团队

ISD Instructional System Design/教学系统设计

ITL Information Technology Laboratory/信息技术实验室

KSA Knowledge, skills, and abilities/知识、技能和能力

LAN Local area network/局域网

NCWF National Cybersecurity Workforce Framework/国家网络空间安全人才框架

NICE National Initiative for Cybersecurity Education/国家标准与技术研究所

OLA Operating-Level Agreement/操作级别协议

OMB Office of Management and Budget/行政管理和预算局

OPM Office of Personnel Management/人事管理局

OS Operating system/操作系统

OSI Open System Interconnection/开放系统互联通信

P.L. Public Law/公法

PCI Payment Card Industry/支付卡行业

PHI Personal Health Information/个人医疗信息

PIA Privacy Impact Assessments/隐私影响评估
PII Personally Identifiable Information/个人身份信息
PKI Public key infrastructure/公钥基础设施
R&D Research and Design/研发
RFID Radio Frequency Identification/射频识别
RMF Risk Management Framework/风险管理框架
SA&A Security Assessment and Authorization/安全评估和授权
SDLC System development life cycle/系统开发生命周期
SLA Service-Level Agreements/服务水平协议

附录 D—参考资料

[1] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0*, http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

[2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, http://csrc.nist.gov/nice/framework/DraftNationalCybersecurityWorkforceFrameworkV2.xlsx

[3] Cybersecurity Framework, National Institute of Standards and Technology [Website], http://www.nist.gov/cyberframework

[4] M. Ennis, *Competency Models: A Review of the Literature and The Role of the Employment and Training Administration (ETA)*, Employment and Training Administration, U. S. Department of Labor, January 29, 2008. https://www.careeronestop.org/competencymodel/Info_Documents/OPDRLiteratureReview.pdf

[5] U.S. Department of Education, Office of Career, Technical, and Adult Education, Employability Skills Framework http://cte.ed.gov/employabilityskills

[6] *Mapping – NSA/DHS Knowledge Unit to NICE Framework 2.0*, National Centers of Academic Excellence in IA/CD, https://www.iad.gov/NIETP/documents/Requirements/NSA_DHS_CAE_KU_Mapping_to_NICE_FW_2.0.pdf

[7] Office of Management and Budget (OMB), *Federal Cybersecurity Workforce Strategy*, OMB Memorandum 16-15, July 12, 2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

[8] U.S. Department of Labor, Employment and Training Administration (ETA) [Website]. https://www.doleta.gov

[9] U.S. Department of Homeland Security, Cybersecurity Workforce Development Toolkit (CDWT), https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

[10] Baldrige Cybersecurity Excellence Program, National Institute of Standards and Technology [Website], https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[11] U.S. Department of Homeland Security, CMSI PushButtonPD ™ Tool Website, https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[12] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[13] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[14] National Initiative for Cybersecurity Education, National Institute of Standards and Technology, http://csrc.nist.gov/nice

[15] Draft NIST Special Publication (SP) 800-160, *Systems Security Engineering -Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2016, 261pp. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_final-draft.pdf.

文档信息	
原文名称	NICE Cybersecurity Workforce 2 Framework (NCWF)
原文作者	Bill Newhouse、Stephanie Keith 、Benjamin Scribner、Greg Witte
原文发布单位	NIST
原文出处	http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf
翻译	湖南合天智汇信息技术有限公司
审核	湖南合天智汇信息技术有限公司
发布日期	2017 年 4 月 18 日
免责声明	1. 原文通过互联网公开方式获得，受翻译水平所限，不能完全保证译文与原含义一致。 2. 译者及合天智汇不对原文及译文中包含或引用的信息真实性、准确性、可靠性提供任何保证。译者及合天智汇不对原文和译文承当任何责任，翻译本文的行为不代表译者及合天智汇对原文持有任何立场。 3. 译者及合天智汇没有与原文作者联系，也没有获得相应的版权授权，译者及合天智汇出于学习目的翻译本文，并无出售、出版译文等任何商业企图，因此不对任何可能因此导致的版权问题承担责任。 4. 本文为合天智汇内部参考文献，主要用于内部交流学习，也向中国大陆境内的网络空间安全领域内的研究人士做有限分享。望尊重译者劳动和意愿，不得以任何方式修改本译文。译者和合天智汇并未授权任何第三方二次分享本译文，因此第三方对本译文所做的分享、报道、传播等行为，及所带来的后果，与译者及合天智汇无关。 5. 本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者及合天智汇一律不予承担。