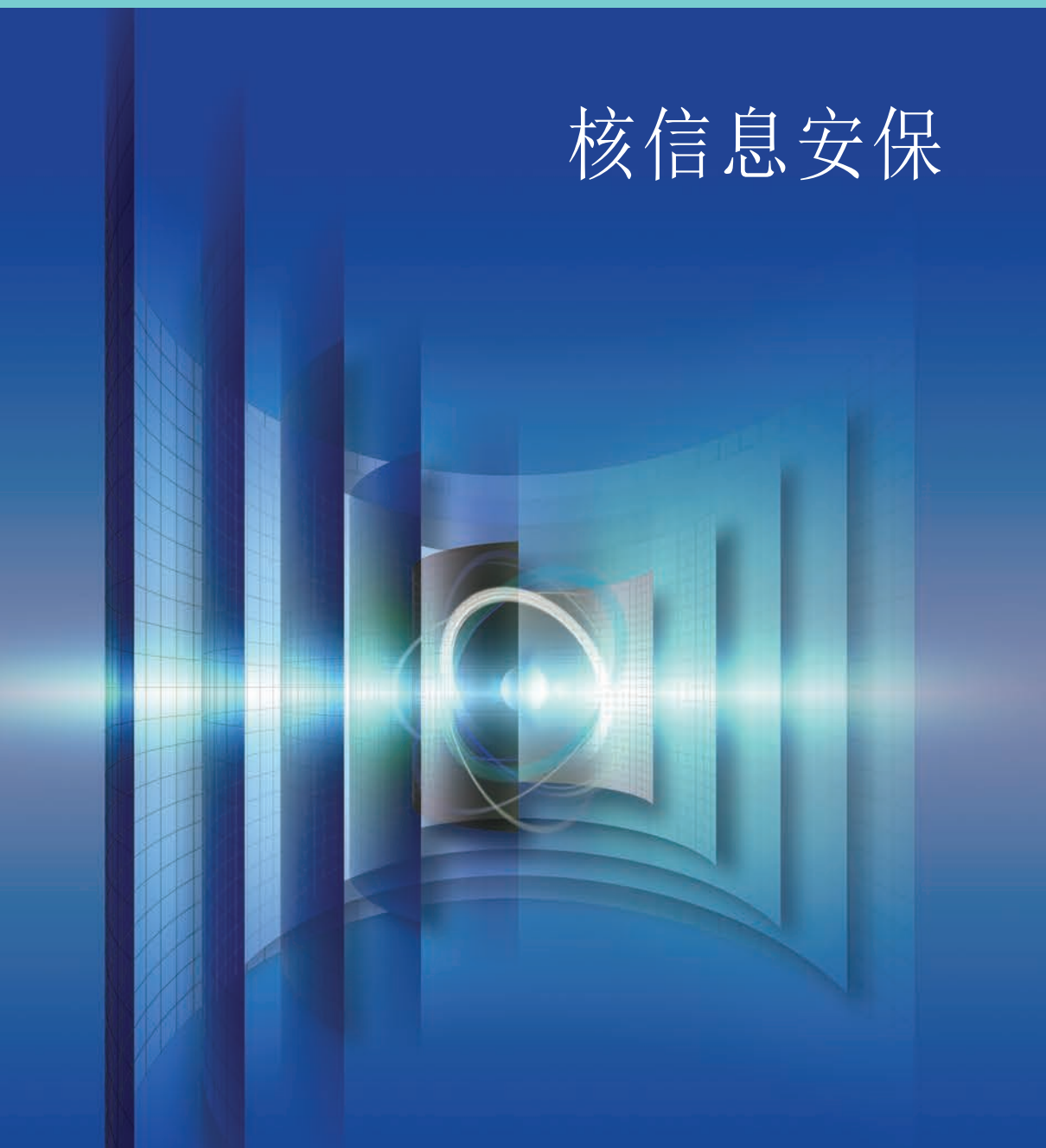
国际原子能机构《核安保丛书》第23-G号

实施导则

核信息安保



IAEA
国际原子能机构

国际原子能机构《核安保丛书》

国际原子能机构《核安保丛书》处理与防止和侦查涉及或针对核材料、其他放射性物质、相关设施或相关活动的犯罪行为或未经授权的故意行为并予以做出响应有关的核安保问题。这些出版物符合并补充国际核安保文书，例如《核材料实物保护公约》及其修订案、《制止核恐怖主义行为国际公约》、联合国安全理事会第 1373 号决议和第 1540 号决议以及《放射源安全和安保行为准则》。

国际原子能机构《核安保丛书》的类别

原子能机构《核安保丛书》出版物按以下类别发行：

- **核安保基本原则**详述国家核安保制度的目标和这种制度的基本要素。这些基本原则构成“核安保建议”的基础。
- **核安保建议**提出国家按照“核安保基本原则”为实现和保持有效的国家核安保制度应当采取的措施。
- **实施导则**就国家可以实施“核安保建议”中提出的措施的方法提供指导。因此，这些导则注重如何落实与广泛的核安保领域有关的建议。
- **技术导则**就具体技术主题提供指导，以补充“实施导则”中提供的指导。这些导则注重如何实施必要措施的细节。

起草和审查

《核安保丛书》出版物的编写和审查涉及原子能机构秘书处、成员国专家（协助秘书处起草这些出版物）以及审查和核准出版物草案的核安保导则委员会。适当时，在起草期间还举行不限人数的技术会议，为成员国和相关国际组织的专家提供机会审查和讨论文本草案。此外，为确保高水平的国际审查和达成高度国际共识，秘书处向所有成员国提交草案文本，以供进行 120 天的正式审查。

对于每份出版物，秘书处都要编写核安保导则委员会在编写和审查过程的相继阶段予以核准的以下内容：

- 说明预定新的或经修订的出版物的概要和工作计划、其预定用途、范围和目录；
- 提交成员国的出版物草案，以供在 120 天磋商期间发表意见；
- 考虑了成员国意见的最终出版物草案。

原子能机构《核安保丛书》出版物的起草和审查过程考虑到机密性，并且承认核安保与总体乃至具体的国家安保关切有着密不可分的联系。

一个基本的考虑因素是在这些出版物的技术内容上应当虑及相关的原子能机构安全标准和保障活动。特别是，在以上所述每个阶段由相关安全标准分委员会以及核安保导则委员会对涉及与安全有接口的领域的《核安保丛书》出版物（称作接口文件）进行审查。

核信息安保

国际原子能机构的成员国

阿富汗
阿尔巴尼亚
阿尔及利亚
安哥拉
安提瓜和巴布达
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴哈马
巴林
孟加拉国
巴巴多斯
白俄罗斯
比利时
伯利兹
贝宁
多民族玻利维亚国
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
文莱达鲁萨兰国
保加利亚
布基纳法索
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
科摩罗
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
吉布提
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
斯威士兰
埃塞俄比亚
斐济
芬兰
法国
加蓬
冈比亚
格鲁吉亚
德国
加纳
希腊
格林纳达
危地马拉
圭亚那
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚
毛里求斯
墨西哥
摩纳哥
蒙古
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
北马其顿
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
卢旺达
圣基茨和尼维斯
圣卢西亚
圣文森特和格林纳丁斯
萨摩亚
圣马力诺
沙特阿拉伯
塞内加尔
塞尔维亚
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
多哥
汤加
特立尼达和多巴哥
突尼斯
土耳其
土库曼斯坦
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
瓦努阿图
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

国际原子能机构的《规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的原子能机构《规约》会议核准，并于 1957 年 7 月 29 日生效。原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《核安保丛书》第 23-G 号

核信息安保

实 施 导 则

国 际 原 子 能 机 构
2023 年 · 维也纳

版 权 说 明

Marketing and Sales Unit
Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 26007 22529
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
https://www.iaea.org/zh/chu-ban-wu

国际原子能机构印制
2023 年 6 月 • 奥地利

核信息安保

国际原子能机构，奥地利，2023 年 6 月
STI/PUB/1677
ISBN 978-92-0-515322-3（简装书：碱性纸）
978-92-0-515422-0（pdf 格式）
ISSN 2790-7023

前　言

根据《国际原子能机构规约》，国际原子能机构的主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。我们不仅要防止核武器扩散，还要确保核技术可以用于健康和农业等和平目的。所有核材料、其他放射性物质以及相关设施均须得到安全管理，并予以充分保护，防止发生违法犯罪行为或未经授权的蓄意行为。

核安保是每个国家的责任。国际合作对于支持各国建立和保持有效的核安保制度至关重要。众所周知，国际原子能机构在促成此类合作和为各国提供帮助方面发挥着核心作用。国际原子能机构的作用反映了其广泛的成员关系、职责和权力、独特的专长以及为各国提供技术支持、专家和实用指导方面的丰富经验。

自 2006 年起，国际原子能机构发布《核安保丛书》出版物，帮助各国建立有效的国家核安保制度。这些出版物是对《核材料实物保护公约》及其修订案、《制止核恐怖主义行为国际公约》、联合国安全理事会第 1373 号和第 1540 号决议、《放射源安全和安保行为准则》等国际核安保法律文件的补充。

国际原子能机构成员国的专家们积极参与编制《导则》，确保其反映各国在核安保问题良好实践上达成一致。国际原子能机构核安保导则委员会成立于 2012 年 3 月，由成员国代表组成，负责在《核安保丛书》编制过程中对出版物草案进行审批。

国际原子能机构将继续与其成员国合作，确保世界各国人民都能享受和平核技术所带来的种种益处，帮助他们提高健康和福祉水平，促进繁荣。

编者按

国际原子能机构《核安保丛书》发布的导则对各国不具有约束力，但各国可利用这种导则协助其履行国际法律文书规定的义务以及在本国范围内履行其核安保责任。用“应当”表述的导则旨在提出国际良好实践和表示对各国有必要采取建议的措施或等效替代措施的国际共识。

安保相关术语按其所在出版物中或该出版物所支持的更高一级导则中的定义加以理解。在其他情况下，词语均按其通常理解的意义使用。

附录被视为出版物的一个不可分割的组成部分。附录中的资料具有与正文文本相同的地位。附件用于提供实例或补充资料或解释。附件不是主文本不可分割的组成部分。

虽已尽力保持本出版物中所载信息的准确性，但是国际原子能机构及其成员国对使用本出版物可能产生的后果均不承担任何责任。

使用某些国家或领土的特定名称并不意味着国际原子能机构作为出版者对这类国家或领土、其当局和机构或其边界划定的法律地位作出任何判断。

提及具体公司或产品的名称（不论表明注册与否）并不意味着国际原子能机构有意侵犯所有权，也不应被解释为国际原子能机构的认可或推介。

目 录

1. 引言

背景

1.1. 国家的核安保体系的总体目标是为了保护人民、财产、社会和环境免受核安保事件带来的有害后果[1]。意欲计划或实施任何涉及核材料或其他放射性物质或相关设施的恶意行为的团体或个人，可能会从获取的敏感信息中受益。因此，应采用适当的措施来识别、分类及保护这些信息。敏感信息是指那些如果未经授权而被披露、修改、变更、销毁或拒绝使用则均有可能会危及核安保的、包括软件在内的任何形式的信息。

1.2. 保密性是指禁止将信息提供或泄露给未经授权的个人、实体或流程。信息安保不仅包括确保信息的机密性，还包括确保信息的准确性和全面性（信息完整性）以及信息在需要时的可访问性或可利用性（信息可用性）。

1.3. 确保敏感信息安保是核安保的交叉前提，制订能有效确保信息安保的制度和措施是国家核安保体系的关键要素。

1.4. 核安保基本法则[1]和所有三篇核安保意见出版物[2－4]都认可保护敏感信息的重要性。本《实施导则》对这些出版物中的高级别陈述进行了扩展，提供了关于应该做什么的更多细节。

目的

1.5. 本出版物为实施保密原则和信息安保等提供了更为广泛的指导。关于建立和管理各类型信息的信息安保框架，国家和国际层面上均提供了很多导则，既包括高级别导则，也包括各种详细的标准。本出版物不打算更改上述导则。相反，其目标在于协助各成员国缩小现有政府和行业标准在信息安保方面的差距，以及适用于核安保的特定概念和考虑因素和在处理核材料和其他放射性物质方面存在的特殊规定和条件之间的差距。

1.6. 本出版物的目标在于就以下方面提供指导：

(a) 建立确保敏感信息机密性、完整性和可用性的有效框架（第 3 部分），包括必要的立法和条例；

(b) 识别可能被视为敏感信息的信息（第 4 部分）；

(c) 关于分享和披露敏感信息的注意事项（第 5 部分）；

(d) 确保机密性、完整性和可用性的指导方针和方法（第 6 部分）。

范围

1.7. 本出版物旨在处理涉及民用核材料和其他放射性物质及相关设施和活动的敏感信息安保问题。侧重于与受监管的材料和设施有关的敏感信息。

1.8. 由于核安保涉及脱离监管控制的核材料和其他放射性物质，也可能涉及需要保护的敏感信息。在这种情况下，这里提供的一般导则均应适用。

1.9. 本出版物的目标受众是负责敏感信息安保的任何人。其中包括：

(a) 主管部门，包括监管机构；

(b) 参与核材料或其他放射性物质使用、储存或运输的设施、公司和组织的管理人员；

(c) 设施运营方及其工作人员，尤其是安保人员；

(d) 为相关部门、组织或设施运营方工作的承包商或其他第三方；

(e) 任何其他可能有权合法获取敏感信息的实体。

结构

1.10. 本部分为引言。第 2 部分会介绍将在整个出版物中使用的几个关键术语和概念。第 3 部分描述了在一个国家内共同构建敏感信息安保框架的必要要素，第 4－6 部分依次论述了这些要素。第 4 部分介绍了确定敏感信息时的注意事项，因此需要对这些信息加以保护。第 5 部分包含分享和披露敏感信息时的注意事项。第 6 部分更详细地介绍了在设施层面为保护敏感信息而采取的必要行动。附件一为分类框架示例。附件二为核安保相关信息安保分类方案的示例。附件三列出了培训和意识大纲的建议格式和内容。

2. 概念和背景

2.1. 本部分阐明了本出版物中使用的某些重要术语的含义。本部分还将信息安保的主要概念应用于核安保的背景介绍中。本出版物最后的术语表中给出了更多相关术语的定义。

信息

2.2. 信息即知识，不论其存在或表达形式是什么。包括想法、概念、事件、过程、思想、事实和模式。信息可记录在诸如纸张、胶片、磁性或光学媒体等材料上，或保存在电子系统中。信息几乎可通过任何手段进行表示和传达。在核领域，存在着形式多样的大量信息。信息资产是用于存储、处理、控制或传输信息的设备或组件（包括媒体）。

2.3. 出于处理和安保的目的，可将信息按信息对象进行分组。可将其定义为对组织有价值的所有信息元素。通常情况下，信息对象包括一般用途、目的、相关风险或存储或传输形式一致的一组数据、信息或知识。

2.4. 核安保相关信息可能对以下某一或所有对象具有价值（可能具有不同的性质和程度），了解这一点很重要：

(a) 国家；
(b) 主管部门；
(c) 设施运营方（包括第三方，如供应商）；
(d) 潜在敌对方（个人和有组织的实体）；
(e) 媒体；
(f) 公众。

敏感信息的识别和保护

2.5. 敏感信息是指信息在未经授权情况下进行披露（或修改、变更、销毁或拒绝使用）可能危害核安保或以其他方式促使针对核设施、组织或运输发生恶意行为。例如，该等信息可能是指设施的核安保安排，设施的系统、结构和组件，核材料或其他放射性物质的运输位置和详细情况，或组织人员的详细情况。

2.6. 识别符合该定义的信息是制订信息安保大纲以确保机密性的关键步骤。第 4 部分提供了有关该主题的更详细和全面的导则，附件二中包含相关例证。

2.7. 保护敏感信息很有必要。如果敌对方轻易就能获取未予充分保护的信息，那么这些信息会帮助其不用冒太大风险便可计划或实施恶意行为。例如，如果某设施的实物保护计划被计划袭击某设施的敌对方获得，该敌对方就会了解到其所面临的障碍、对方警卫部队的多少和武装准备、快反部队的规模大小，以及部队到达现场大致需要花费的时间，而且会知道设施内的重要目标及其位置和采用的保护措施。同样，如果一个想在运输过程中窃取核材料的敌对方成功获得了一部能够获取有关计划运输详细信息的设备 — 只因该设备未得到充分的保护，敌对方即可更有效地计划攻击行为。因此，敌对方获取这些信息或信息资产会增加其成功的可能性。

2.8. 访问敏感信息和敏感信息对象的范围不应超过组织业务所需的范围。由此可以推断：信息传播应仅限于那些获得适当授权的个人，且仅限于那些需要访问的情况。“需要知道”和“需要持有”这两个规则是确保敏感信息安保的基本要求。信息访问权应在这些规则指导下进行管理和控制。访问权应定期审查，并在必要时进行审查。

2.9. 确保机密性取决于对选定的敏感信息和敏感信息资产（用于处理、运用、存储或传输敏感信息的设备或组件，包括媒介）所采用的安保措施，以确保其不会落入未经授权的内部或外部个人或组织手中。针对内部威胁应采取措施的导则载于《内部威胁预防和保护措施》[5]。安保措施应基于风险分析确定。风险分析应通过定期审查保持更新。

信息安保

2.10. 如本出版物所述，信息安保是指为确保任何形式的信息的机密性、完整性和可用性而制订的制度、大纲或规则。至少包括：

(a) 任何实物形式的信息安保（如纸质和电子媒介）；

(b) 计算机系统安保，有时称为计算机安保、信息技术（IT）安保或网络安保（可在《核设施计算机安保》中找到国际原子能机构提供的其他导则[6]）；

(c) 信息资产（如信息存储和处理设备/通信系统和网络）安保；

(d) 有关设施雇员和第三方（如承包商和供应商）的信息安保，且其可能危及上述安保；

(e) 无形信息（如知识）的安保。

2.11. 虽然保密性往往会单独提供保障，但各组织应确保其信息安保大纲能够解决所有三个方面的问题。丧失完整性或可用性可能会对核安保造成负面影响，就如同保密性可能会丧失一样。例如，如果授权用户未能及时获取其职责所必需的信息（可用性丧失），或者信息因被改变而对其产生误导（完整性丧失）。

2.12. 应在总体安保框架范围内考虑并应用信息安保。其与实物保护和人员安保等其他安保领域密切相关。例如，实物保护措施可用来保护敏感信息和敏感信息资产，而保密措施则会使敌对方更难或更无法确定如何对实物保护系统发起攻击。任何安保领域存在差距或不足都可能影响到其他安保领域的安全性，所以使用考虑所有领域后的综合方法至关重要。

2.13. 信息安保还应考虑安全与其他目标之间的必要平衡，包括安全性、开放性和透明度以及运营方面。国际原子能机构《安全标准丛书》为安全提供了指导。

3. 保护敏感信息的框架

3.1. 在分散的设施基础上保护敏感信息不会取得任何效果。有必要采取有效的国家框架来确保所有设施、场所和组织（政府和非政府组织）在处理敏感信息时采取全面的安保措施。成员国应建立国家框架，其中包括确立：

(a) 成员国责任；

(b) 法律和监管框架；

(c) 国家导则；

(d) 安保政策；

(e) 分类方案。

各组织内部的政策也应为整体框架提供支持。

职责

3.2. 成员国政府应负责建立其综合核安保体系并保障该体系的有效运行。保障敏感信息安保是成员国应执行的核安保体系的一个主要部分。

3.3. 各成员国通常设有负责国家整体安保的政府组织或机构，以下简称国家安保部门。国家安保部门通常负责确定安保各方面的基本国策。国家安保部门发布的安保政策和指示往往具有通用性，而非专门针对核安保而制订。但是，许多成员国的国家安保部门确实针对敏感信息保护提供了政策和导则，例如针对政府或军事用途的情况。

3.4. 成员国有关主管部门应制订和发布针对核材料及其他放射性物质相关设施和活动方面的敏感信息安保的政策和要求。这些通常基于国家安保部门发布的国家安保政策和要求而制订，但要考虑到涉及这些材料的活动的特殊性。主管部门还应与国家安保部门保持密切联系，以确定国家威胁评估或设计基准威胁（更多信息参见《制订、使用和维护设计基准威胁》[7]）。

3.5. 各组织应制订其内部政策、计划和程序，从而确保其控制或处理的核安保相关敏感信息的机密性、完整性和可用性，并根据国家安保政策和相关国家法律和要求保护相关的敏感信息资产。所有员工都应充分认识到信息安保的必要性，并遵循组织的信息安保规则和程序。

保护敏感信息的法律和监管框架

3.6. 维护国界内核安保的要求应适用于所有部委、部门、机构和其他组织，其负责处理国家认定的国家核安保所必需事项。成员国可通过法律、法规或其他具有法律约束力的要求强制执行这些要求。成员国对核安保的要求应包括信息安保要求。还应制订立法，对违反此类信息安保要求的任何个人或组织实施制裁或处罚。此类立法的某些章节可能对违反特定类型保密性或其他信息属性及相应制裁的严重性进行了阐释。

3.7. 主管部门应拥有监管权力可要求敏感信息持有人承担相应义务。应根据为此目的制订的法律对未经授权的信息披露行为进行制裁或惩罚。立法还应当要求成员国各部委、部门、机关和其他组织向主管部门提供一切必要的支持，使其能够履行保证敏感信息安保的任务。

制订国家级导则

3.8. 成员国关于信息安保的政策应当确定成员国希望保护的信息类型，并说明如何实施这种保护措施。这通常在国家安保部门（或其他有关部门）编制的安保手册中列出。此类手册可能不会直接提及核安保的敏感信息。但是，此类手册会对不同类别的信息进行说明，规定其敏感程度和因此确定的安保等级，以及如何标记信息对象才能确保其敏感程度显而易见。

3.9. 有关主管部门应与国家安保部门密切联系，并在核材料和其他放射性物质使用方的参与下，针对敏感信息的构成提供详细指导。此类导则通常以国家威胁评估规定为基础，并应与其保持一致。此类导则（有时称为分类政策）通常将信息类型划分为一系列相关主题，并指出特定信息的相对重要性，从而指出其敏感性和采用的安保程度。

3.10. 在组织层面，特定信息的重要性可以在组织的安保计划中加以说明。此类安保计划应说明如何根据国家立法和法规保护特定的敏感信息。

安保政策

3.11. 除发布符合国家要求的信息安保政策之外，主管部门还应提供详细信息来说明这些要求如何适用于涉及核材料和其他放射性物质的设施和活动。

3.12. 成员国的核安保政策应表明对信息安保的承诺。为对此进行鼓励，可发布和维护适当的综合信息安保政策以用于所有涉及核材料和其他放射性物质的设施和活动以及任何其他储存有关敏感信息的地点。此类政策的目的在于确保敏感信息安保，防止信息泄露。

3.13. 负责处理敏感信息的各组织和机构都应根据主管部门提供的适用的政策编制自己的专用信息安保政策。此类政策应采用与目标用户相关且易于获取和理解的方式在整个组织内进行传达。第 6 部分包含有关建立信息安保管理大纲的其他导则，其中包括政策。

信息分类方案

3.14. 实施信息安保计划和相关控制程序需要资源和时间。在某一地点或设施中同等程度地保护所有信息既不可行有时也不可取。有些信息并非敏感信息，因此不需要任何特别的保证措施。即使对于敏感信息，不同的信息对象也可能需要不同的保护级别。因此，识别哪些信息是敏感信息及其需要哪种保护级别非常重要。各国主管部门应确定哪些有关核材料、其他放射性物质、相关设施和活动的信息属于敏感信息。关于国际运输方面，成员国应确定哪些信息需要进行保护，并可能要考虑到与参与国际运输的其他成员国达成一致。

3.15. 评估特定信息资产的价值时推荐采用风险知情方案，同时考虑到信息泄露情况下可能造成的危害和后果。需要指出的是，关于某一设施的任何信息泄露都可能会影响具有类似信息资产的其他设施；因此，对于其他地点对核安保产生的影响，应广泛考虑其损害和后果，而不仅仅是针对某一特定地点。应特别考虑信息的积累和潜在的单点故障（例如依靠单一网络或电力供应的信息资产）。根据特定成员国使用的分类制度，可通过评估结果来确定每一个信息对象所需的必要保护等级。

3.16. 应建立和维护国家分类制度，将信息划分成不同的类别，这样在一个类别内未经授权披露任何信息会产生类似的结果，因此特定类别的所有信息都应遵守类似的安保要求。应将其确定为国家制度，而非特别针对某一特定行业或由单一设施而设计的制度。许多情况下，各成员国已维持这种分类制度，但是这种制度可能无法解决特定的核安保信息问题。该制度基于风险知情方案制订，其中未经授权披露信息造成的潜在后果决定了这类信息的类别和相关安保要求。

3.17. 应仔细考虑分类类别的数量以及从其使用中获得的好处。方案过于复杂可能会导致操作困难且不切实际，而方案太过简单则可能无法确保分类的精确性。此外，为各信息对象指定分类级别时也应谨慎。过度分类（即要求的安全性比真正需要的更严格）可能导致产生不必要的额外费用，而分类不足则可能会使信息产生极大的泄露风险。过度分类也可能会与透明度政策相冲突，或造成分类对于信息使用方来说意义不大的情况。

3.18. 敏感信息可能采用的分类方案（其类别表示特定信息对象的敏感性）可能包含以下级别[1]：

(a) **保密；**

(b) **机密；**

(c) **限制级。**

3.19. 附加信息标签可能提供了对信息分类引起的信息分发进行的限制，例如：

(a) 不进一步分发；

(b) 发起人对分发进行控制；

(c) 官方使用；

(d) 限制分发；

(e) 可供公众使用。

3.20. 附件一中给出了分类等级（从保密到限制级）的示范性定义。

4. 敏感信息识别

4.1. 对信息进行分类和保护的第一步是识别被视为敏感信息的信息。

4.2. 对于可能影响核安保的以下类型的信息，应考虑对其进行安全管制[2]：

(a) 有关核材料、其他放射性物质、相关设施和活动的实物保护系统和任何其他安保措施的详细信息，包括警卫和快反部队的信息；

(b) 关于使用或储存的核材料或其他放射性物质的数量和形式的信息，包括核材料衡算信息；

(c) 有关运输中的核材料或其他放射性物质的数量和形式的信息；

(d) 计算机系统（包括通信系统）的详细信息，系统用以处理、运用、储存或传输对安全和安保直接或间接重要的信息；

---

[1] 在很多成员国，关于绝密还有进一步的分类。大多数成员国的民用部门几乎从未使用过这种分类级别。其通常适用于军事和武器部门。

[2] 该列表并不包括所有这些可能的情况，但可提供起点以供考虑。

(e) 核安保事件的应急响应计划；

(f) 有关员工、供应商和承包商的个人信息；

(g) 威胁评估和安保警报信息；

(h) 敏感技术的详细信息；

(i) 与上述主题相关的漏洞或弱点的详细信息；

(j) 有关以上任何主题的历史信息。

上述某些信息（如个人信息）也可能受到其他国家法律或公司政策的特定安保要求的限制。

4.3. 附件二第 4.2 段类别中包含下列特定类别信息的示例，从而表明其是否通常被视为是敏感信息，以及相关原因。

5. 敏感信息共享和披露

5.1. 敏感信息常常需要不断进行合法的分享，例如在适当的国家机构之间分享、在处理核材料或其他放射性物质的组织和有关主管部门之间分享，或不同的成员国之间进行分享。同样，有时还需要临时向其他组织或公众披露敏感信息。信息的分享和披露均应进行管理，以确保敏感信息不会被无意中分享或披露给那些不需要知道的人员。

信息分享

5.2. 有时需要将某些敏感信息与授权的国家机构或需要了解该信息的公司和组织分享。信息分享可提高效率，如果要独立编制和处理这些信息，效率则无法提高。另外某些情况下，不分享信息可能会损害安保或者削弱安保措施的总体规划、设计和实施。此外，由于核安保责任往往并非由任何一个单一的机构、公司或组织承担，因此通常有必要将信息共享给分担安保责任的所有相关方。例如，为了国家安保，主管部门通常需要将敏感信息传递给国家安保部门，反之亦然。例如，应及时将威胁评估的变化或安保事件的信息传达给相关机构以便能够调整安保措施并交流操作经验，以此作为持续改进的基础。除安保方面的考虑之外，可能还需要共享信息以为其他目标提供支持，包括安全评估、运营和商业需求。

5.3. 信息分享的性质和范围首先应遵循国家法律或法规，然后在共享的好处和安保的需要之间取得平衡。有关部门之间进行信息传递应遵循的规则应根据该国的安保程序进行控制。建立成员国内部通用方法可确保敏感信息不会在不适当情况下披露。

5.4. 某些信息通常也有必要分享给其他成员国或有关国际组织这种情况下，应该制订某种协议来保证接收方能按信息所有人要求的方式保护敏感信息。可通过双边或多边条约或协议来保证信息安保，这些条约或协议规定了如何保护信息免于被披露。这种协议通常会提供必要保护措施用于保护各成员国不同分类级别的敏感信息。此外还应考虑到任何一个成员国的特殊要求（如信息自由立法，见第 5.6 段）是如何影响到对其他成员国敏感信息的处理的。

信息披露

需要披露

5.5. 大多数成员国都制订了法律来确保对国家利益较为重要的信息的安保。这些法律规定，如果一个人（该国或其他成员国的国民）违反了有关此类信息机密性的法律，那么其将得到制裁。通常还会制订法律以规定个人是否有权获得官方的政府信息。还可能会提供机制来解决政府和其他各方为保护成员国安保而不能提供哪些信息而出现的分歧。

5.6. 有几个成员国拥有信息自由立法或其他法律，允许公众要求获得有关部门掌握的信息。通常情况下，有关部门可能唯一会保留的信息属于指定豁免所涵盖的信息类型，例如与国防有关的信息，或私有和个人信息。对于一些成员国，其带有分类标志的物品不会自动免于披露。

5.7. 其他法律和法规可能会要求披露某些类型的信息，其中可能包括敏感信息。例如环境立法要求公开报告具体的信息。应确保这些法律允许不披露可能影响成员国安保或第三方安保的信息。

关于披露导则的编制

5.8. 应制订具体的导则来协助组织和机构决定哪些敏感信息可以披露。在编写这些导则时，责任政府机构通常会咨询其他政府部门和相关组织。导则可确定其认为不适合披露的信息类型，其目的应该是防止未经授权披露敏感信息（另见附件二）。

5.9. 各成员国有必要就以下方面提供具体指导：

(a) 根据信息披露造成的后果，确定某些类型敏感信息的敏感性；
(b) 哪些类型的信息可以披露，在哪些情况下，向谁以及通过哪些特定的方法披露；
(c) 信息披露的条件；
(d) 在公开发表之前审查信息潜在敏感性的过程，例如在会议演示文稿、网页帖子或技术规范中；
(e) 在未经授权披露敏感信息（不论有意或无意）或其他违反信息安保要求的情况下，应采取哪些措施。

5.10. 导则随时会发生更改。随着情况不断发生变化，可能被认为敏感的信息和不适合一次性完全披露的信息可能会不再那么敏感，适合稍后披露（反之亦然）。因此，在政策或情况发生重大变化的情况下，应定期审查和更新导则。

5.11. 通常情况下，可以在适当情况下降低适用于特定信息的安保级别。但是，如果信息已经被广泛披露，那么将信息重新分类到一个更受限制的类别可能无法实现或者也可能不起作用。在原来的分类中应该考虑到这一点，且应考虑到适当平衡保密性和谨慎性，以及可用性和透明度。应制订分类定期审查的默认时限，但也应在需要时做出更改，例如情况发生重大变化时。

5.12. 应按照相同的导则或标准来考虑所有向组织要求披露敏感信息的请求。如果可能，应由单独的中央办公室来处理所有该类请求。通常用来获取敏感信息的不当访问技术是指向同一组织内的不同个人或单位发出多个请求。如果不进行协调即分开处理此类请求，则可能会给出不同的回应，并且可能会披露原本不会被披露的敏感信息。

6. 保密性管理框架

6.1. 第 3 部分对保护敏感信息的高级框架进行了说明。本部分更详细地阐述了在设施或组织内所需的这种框架的各组成部分，并将其放在管理制度的背景下进行说明。

6.2. 应建立一套管理制度，制订政策和目标，并以高效且有效的方式实现目标。综合管理制度（见国际原子能机构《安保标准丛书》第 GS-R-3 号《设施和活动管理制度》[8]及相关导则）是核安保文化的重要支持要素。设施中的许多活动均由管理制度来控制。将安保、安全、健康、环境、质量和经济要素理想地整合到一个单独的管理流程或一套综合的且相辅相成的制度中。应将信息安保融合到设施或组织的现有管理制度中，以确保信息的机密性、完整性和可用性。

6.3. 确保敏感信息的保密性、完整性和可用性取决于有效地指定角色并确定责任，进行分类以确定哪些信息是敏感信息且需要进行保护、为何这些信息需要保护以及采用何种级别的保护（见第 4 部分），做出决定以确定如何获取这些信息，实施必要的安保措施，以及在这些信息被泄露、盗取或丢失的情况下，应如何应对（包括恢复）。

6.4. 在下文进行解释的管理框架适用于控制或处理敏感信息的组织的各级管理层。

职责

6.5. 管理层负有全面责任，确保信息安保在整个设施或组织内得以落实且有效实现，从而保护敏感信息。负责处理敏感信息的所有人员均有责任根据相关的国家立法和组织的政策和程序确保其安保。

管理层职责

6.6. 管理层职责通常包括：

(a) 承担保护敏感信息和敏感信息资产的全面责任；
(b) 确保遵守相关法律法规；
(c) 指定组织安保责任；

(d) 提供有效的安保培训和教育；

(e) 确保制订有效的信息安保政策；

(f) 提供足够的资源来实施有效的信息安保大纲；

(g) 确保制订信息安保大纲并编制相关计划和程序；

(h) 确保对计划、程序和政策进行有效的变革管理；

(i) 确保对信息安保政策和程序进行定期审计、审查和修订。

分类责任

6.7. 有关主管部门应以分类导则或指南的形式针对信息对象的分类提供指导。此类文件会将特定主题的信息进行分组，并指出信息的敏感性。最初提供敏感信息的人员应使用该导则决定适当的分类级别。

6.8. 一旦信息开始传播，未经原始信息提供方许可，敏感信息对象的接收人或持有人不得改变适用于信息的分类级别。副本的接收人和持有人在适当情况下可以对所适用的分类级别提出质疑。例如，如果主管部门收到运营方发来的信息，并且参考适用的法律后发现信息分类错误，则应指示运营方更改分类。

6.9. 在原始信息提供组织不再运作的情况下，其接任人将成为责任方。但在无法追查到接任人的情况下，敏感信息对象的持有人经与有关主管部门协商后，可酌情改变其分类级别。

6.10. 如果适用于信息对象或信息对象类型的分类级别发生变化，则应尽可能通知所有可能受到影响的人员。这可能包括当前和过去的信息持有人以及将来可能使用该信息的人员。

安保计划

6.11. 所有处理敏感信息的组织均应制订安保计划。安保计划应包含详细的章节专门处理敏感信息安保问题。应将针对安保计划的相关要求传达给为组织工作的员工和承包商。员工和承包商需知晓自己的责任，这一点至关重要。

安保政策和程序

信息安保计划

6.12. 组织的政策和程序分级系统中应包含针对信息安保应担负的责任。至少应解决以下问题：

(a) 有关信息安保的定义及其总体目标、范围和重要性的说明。

(b) 角色和责任的定义，包括设立负责指导和管理信息安保的联络点。

(c) 遵守信息安保要求，包括法律、监管和合同要求。

(d) 制订风险管理计划，基于风险评估法采用适当的控制措施，将风险降至成员国规定的可接受水平。对于核设施，风险管理计划应得到主管机关或成员国指定的其他机构的批准。

(e) 定期监督和审查现行安排，确保政策、标准和程序保持相关性和有效性。

(f) 提出针对教育和培训的要求，确保工作人员、承包商和其他人员对其职责所需的政策、程序和做法有恰当的认识，并充分理解各自应担负的责任（包括其法定义务）。

(g) 违反信息安保要求造成的后果（即处罚或制裁）或在保护敏感信息时出现的故意疏忽。

(h) 为政策提供支持的参考文档，例如有关用户应遵守的特定制度或安保规则的更详细程序。

针对敏感信息的信息安保计划

6.13. 具体提及敏感信息保护时，计划还应包括：

(a) 信息生命周期：对创建、识别、分类、标记、处理、使用、存储、传输、重新分类、复制和销毁敏感信息的过程进行定义；

(b) 针对敏感信息的安保要求，应适当考虑信息的机密性、完整性和可用性等安保目标；

(c) 获取敏感信息和敏感信息资产的机会限于需要该获取机会履行职责的人员。这些人员拥有必要的权限，并且要经过与信息分类等级相称的可信度检查；

(d) 敏感信息所采用的传输方式应确保将泄密风险、未经授权的拦截、修改或干扰降低到可接受的水平。

处理敏感信息的程序

6.14. 对信息的机密性、完整性和可用性的威胁风险进行有效管理，其中将涉及针对这些威胁制订有效的对策。该过程必然涉及对信息安保、实物保护和人员安保等方面进行综合的安保控制。

6.15. 人员安保，包括可信度检查，可确保那些获得敏感信息的人员经成员国确认为相对可被信赖。对于分类等级相对较低的信息，组织应决定是否需要对那些需要访问信息的人员进行检查；如需要，则只需对其个人背景进行有限检查即可。获取更高分类等级的信息时，需要进行更全面的背景调查来确定人员可信度。人员安保程序中还应包括执行人员与主管部门或相关组织之间签订的保密协议。

6.16. 实物保护通常将通过对安保边界进行严格的控制管理与靠近信息资产（例如金库和其他安保位置）的一层或多层其他实物保护措施相结合。可采用相同的原则为信息和信息资产提供实物保护。

6.17. 信息安保措施包括对信息对象整个生命周期进行的技术、程序和行政控制，包括创建、处理、存储、传输、复制和销毁。信息安保措施包括：

(a) 对管理、维护和发展信息安保（包括第三方服务）的行政管理；
(b) 人员安保，尤其是在招聘阶段和上岗开始和结束阶段；
(c) 使用、处理或放置敏感信息或敏感信息资产的各区域实物安保；
(d) 数字和手动处理信息的安保：工作站安保，病毒和恶意软件防护、信息的删除和销毁以及手动处理过程；
(e) 通信网络安保（电话、电子邮件、互联网和局域网）：政策、用户认证、设备识别、隔离、连接和路由控制以及监控；
(f) 设备安保：出入口控制、使用记录、备件管理、关键设备备份、备用电源安排、建档和维护、布线和媒介安保；
(g) 软件安保：出入口控制、用户和超级用户活动记录、备份管理、维护合同签署、配置和版本管理、使用注册的合法软件、测试漏洞以及在错误情况下测试系统行为；

(h) 信息系统的安保使用：用户权限控制、用户识别和验证、连接到服务、系统和设备、密码管理、使用监督和针对关键操作的双人规则（即双人控制）；

(i) 信息处理的分类和相应程序；

(j) 隐私保护。

6.18. 处理敏感信息时应按照国家安保政策和导则的信息安保部分的程序进行管理，包括国家主管部门对其进行的任何解释。信息安保计划中应对各种安保级别的最低性能标准进行说明。比如用于电子信息传输的加密方法。

权限管理制度

6.19. 应建立管理制度，以便对敏感信息的具体持有人和使用人应该通过何种方式、出于何种原因以及在何时可得到授权访问敏感信息和敏感信息资产等进行控制。权限管理制度通常包括：

(a) 确定的授权管理责任结构；

(b) 确定的职能程序，有权指定某人且其自身有权访问敏感信息和敏感信息资产；

(c) 确定的职能程序，指定如何验证、控制和监督访问指定功能；

(d) 确定的程序可决定访问敏感信息和敏感信息资产的授权能持续多久；

(e) 确定的程序可取消访问敏感信息和敏感信息资产的授权；

(f) 确定的程序，在管理链的所有步骤中可保持对权限管理的完全可追溯性，从而授权访问敏感信息和敏感信息资产。

定期审查

6.20. 安保政策、计划和程序应根据情况的不断变化进行调整。确保其不断保持更新的有效方法可能是在政策文件中添加审查时限。如果情况发生根本变化，且可能导致政策改变，例如立法出现变化，那么审查可以提前进行。审查结构应适用于针对核安保责任的各级政策。

安保文化

6.21. 发展、培育和维护强有力的核安保文化是核安保体系的重要组成部分。在信息安保方面尤其如此，人员和流程往往是保护信息安保的关键因素。

6.22. 作为有效核安保文化的一部分[9]，所有组织、雇员和承包商均应充分了解其各自的核安保责任和这些责任的重要性。员工和承包商必须接受与其个人职责和需求相对应的安保教育和培训。

6.23. 承担具体安保责任的员工和承包商和有权获得敏感信息的人员，以及组织内各级管理人员均需针对其职责接受具体的培训并了解情况说明。确保负责处理敏感信息但不必知道信息内容的其他类别的员工（例如通信员、安保人员和办事员）也应接受针对其职责的安保培训。

6.24. 一次性信息安保培训活动不足以巩固培训内容，且长期以来可能会使员工安于现状。负责处理敏感信息的每一个人，包括所有管理层、员工和承包商，都应不断接受在职培训，并定期参加进修课程。所有员工和承包商接受和完成的正式培训记录应予以保存。所有相关雇员和承包商应尽快知悉安保规则和程序出现的任何变化，这一点尤其重要。附件三列出了培训和认识大纲的建议格式和内容。

针对第三方的信息安保安排

6.25. 主管部门或组织有时需要第三方提供涉及敏感信息的服务或商品。应通过法律协议确定此类安排，如许可证或合同，包括保密协议。根据与第三方达成的协议，敏感信息可能会交由第三方处理。为确保这些信息得到保护，应制订涉及敏感信息安排的国家政策或立法。那么合同签约组织和设施就有义务遵循该政策。

6.26. 在与第三方进行谈判时，签约组织有责任确保委托给第三方的敏感信息得到充分的保护。旨在保护敏感信息的安保措施与风险相一致并符合政策要求。

6.27. 在这种情况下，主管部门和组织应确保第三方：

(a) 拥有至少符合组织自身安保安排要求的信息安保流程和程序；
(b) 提供联络点来指导和管理签约公司的安保事宜；
(c) 建立适当的系统，确保对有权查阅第三方所掌握的敏感信息的所有工作人员均进行适当级别的可信度检查；
(d) 确保只允许有必要知道且拥有适当安保许可的人员获取敏感信息和敏感信息资产；
(e) 应采用符合国家立法和地方政策的方式传递信息，防止信息出现泄露风险；
(f) 确保不与任何未经授权的各方或个人共享信息；
(g) 确保所有人员具备适当的安保政策和实践意识，充分理解其各自的责任（包括各自的法律义务）；
(h) 拥有处理信息安保事件的程序；
(i) 确保主管部门或缔约组织按照协议的规定定期检查第三方场所的安保措施安排，确保其符合协议规定的安保要求。

检查和审计

6.28. 定期开展保证活动对于维持信息安保大纲来说至关重要。需要保证持有敏感信息的组织（包括第三方在内）所实施的安保大纲各方面全部符合国家政策和法规。适当情况下，信息安保措施应由主管部门进行审查，然后方可获得正式批准。可通过定期、正式的检查或组织或设施施行的审计来提供保证。审计通常在组织内部进行，而检查在内部和外部均可进行。此外，检查可公布可不公布（即发出或不发出预先通知）。

6.29. 内部检查和审计由组织实施，以确定所指定的安保大纲是否符合已经批准的信息安保大纲，并确保其符合监管要求。进行这类检查有助于组织相比外部检查而言更加频繁地检查自己的合规性。此外，熟悉内部要求、程序和制度的人员进行检查或审计时发现的改进机会可能会与外部检查可能发现的有所不同。

6.30. 外部检查由主管部门或其他获得授权的外部组织实施。检查的目的在于评估国家信息安保政策的合规程度。与组织自己进行的检查相比，外部检查会提供独立的评估。使用外部审计人员时，应处理好保密性和可信度问题。

6.31. 检查和审计结果应重点突出具体需要行动或改进的领域。应为已经确定的预防和纠正措施指定具体的时限，从而便于措施的纠正或实施。应跟进纠正和实施措施并评估其有效性。

信息安保事件

6.32. 泄露信息对象可能导致违反安保规定。信息泄漏时出现的两种违规类型包括泄漏和丢失。泄露通常与未经授权披露、故意或意外泄漏信息的情况下出现的泄密有关。丢失通常与信息或信息资产的被盗或未能得到适当保护所导致的信息泄露有关。

6.33. 信息安保事件也可能涉及到信息丧失可用性或完整性，其可能因无意或有意的行为而造成。例如，如果信息系统（如数据库）出现故障或恶意拒绝服务（故意干扰具有过多数据流量的信息网络），则可能导致信息可用性的丧失。例如，如果信息系统损坏、数据库破坏或在传输过程中未经授权而改变信息，都有可能导致信息完整性的丧失。

6.34. 向主管部门报告重大事件或违反核安保的行为（包括违反信息安保的行为）具有强制性，这一要求应在国家法律法规中予以体现。法律法规还应规定对未作报告的行为进行制裁或处罚。

6.35. 组织和设施负责人应提供正式的报告安排，以确保其能立即了解所有的信息安保事件，以便采取纠正行动，并酌情向主管部门报告事件情况。任何人不得以情况窘迫为借口而不报告任何级别的信息安保事件，一旦发生事件应立即报告，这样方可采取适当的纠正措施并确定事情发展趋势。

调查

6.36. 应对所有信息安保事件进行调查。应制订相应的政策和程序对信息安保事件调查进行控制。调查的目的应该是确定安保事件是否会对信息安保和保密性产生轻微或重大的影响。主管部门随后可采取适当的行动。例如，一件微小事件可能导致文件不能得到正确的锁定或保护，但不会导致任何信息的丢失或泄露。但是，如果是一件重大事件，则可能会致使安保计划被盗，从而对组织构成战略威胁。

6.37. 调查应该：

(a) 充分考虑事件发展的情况，从而确定事件的范围、规模和影响。
(b) 评估事件的后果和可能发生的泄密程度。
(c) 评估是否需要采取进一步的行动或更广泛的调查，可能会涉及到其他机构。
(d) 推荐纠正措施或采取措施控制影响或尽量减轻后果。
(e) 报告调查结果，包括：

    (i) 导致事件发生的可能原因；
    (ii) 评估的泄密程度；
    (iii) 泄密可能产生的影响；
    (iv) 关于改进安保大纲可能提供的意见，以避免类似的事件发生；
    (v) 针对事件所推荐的进一步行动；
    (vi) 有关方需要从中吸取教训。

6.38. 主管部门应当记录所报告的信息安保事件的数量和类型。应确定安保故障会出现的再发事件或趋势，并可能需要更改安保策略或改进安保程序或大纲。更新的趋势和变化也应包含在意识培训内容中，这样才能使员工和承包商掌握准确的安保文化知识。组织和设施也应该保留自己的记录。

参考文献

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

附 件 一

分类制度和定义

I-1. 附件一为分类框架示例。各国可设计和采用任何适当的分类制度来表明核安保信息的敏感程度。下文给出的定义所代表的四级制度与许多成员国的类似。第四级绝密尚未讨论。因为经验表明，民用核领域的信息资产不可能涉及绝密分类。同时应该注意的是，尽管我们将信息主要设想为文件或知识的形式，但是对设备或其他实物对象的内部或外部外观、结构、操作、测试、运用或使用进行视觉观察时也可以从中推导出分类信息，这时就有可能对设备或其他实物对象的各项信息进行分类。

秘密级

I-2. 归类为“秘密”的信息或材料泄露可能会：

(a) 恶化国际紧张局势；
(b) 严重损害政府之间的关系；
(c) 直接威胁生命，或严重损害公共秩序或个人安保或自由；
(d) 严重破坏国家安保部队的作战效能或安保，或者破坏极为重要的安保或情报收集活动的持续有效性；
(e) 对国家财政或经济和商业利益造成重大损害；
(f) 会对策划恶意行为的个人或团体起到帮助作用，而后者的行为可能会对具有核材料或其他放射性物质的设施或在核材料或其他放射性物质在运输过程中对设施造成严重损害。

机密级

I-3. 归类为“机密”的信息或材料泄露可能会：

(a) 损害外交关系；
(b) 损害个人安保或自由；

(c) 造成国家安保部队的作战效能或安保受损，或者破坏具有价值的安保或情报收集活动的有效性；

(d) 严重损害国家财政或经济和商业利益；

(e) 极大地削弱重要组织的财务可行性；

(f) 妨碍调查或者促使重大犯罪行为的发生；

(g) 严重阻碍政府重大政策的制订和实施；

(h) 阻止　或以其他方式严重扰乱重要的国家行动；

(i) 会对策划恶意行为的个人或团体起到帮助，其行为可能会对具有核材料或其他放射性物质的设施或在核材料或其他放射性物质运输过程中对设施造成严重损害。

限制级

I-4.　归类为“限制级”的信息或材料泄露可能会：

(a) 对外交关系造成不利影响；

(b) 给个人造成实质性的困扰；

(c) 使得更难以维护国家安保部队的作战效能或安保；

(d) 可能会对个人或公司的财务或盈利造成损失，或助其获取不正当收益或利益；

(e) 妨碍犯罪调查；

(f) 促使犯罪行为的发生；

(g) 违反确保第三方提供的信息保密性的承诺；

(h) 阻碍政府各项政策的有效推进或实施；

(i) 违反对信息披露的法定限制；

(j) 使政府在与他方进行商业或政策谈判时处于劣势；

(k) 破坏对公共部门及其运作的妥善管理；

(l) 会对策划恶意行为的个人或团体起到帮助，其行为可能会对具有核材料或其他放射性物质的设施或在核材料或其他放射性物质运输过程中对设施造成严重损害。

I-5. 根据上述分类等级对核敏感信息进行控制时，应考虑未经授权披露此类信息会如何帮助潜在的敌对方实施下列行为：

(a) 实施盗窃或破坏核材料或其他放射性物质、设备或设施的行为时选择目标。

(b) 计划或实施盗窃或破坏核材料或其他放射性物质、设备或设施的行为：

(i) 安保系统的设计；

(ii) 制订计划；

(iii) 对核材料或其他放射性材料进行转移、衡算和处理时采用的方法和程序；

(iv) 安保计划、程序和能力。

(c) 衡量盗窃或破坏核材料或其他放射性物质、设备或设施的行为是否成功：

(i) 破坏特定重要设备或设施时造成的实际后果或假设后果。

(d) 非法制造核爆炸装置、放射性散布装置或辐射曝露装置：

(i) 用于编制设备的设计信息；

(ii) 制造设备所需材料的位置；

(iii) 核武器的位置。

(e) 在环境中散布核材料或其他放射性物质：

(i) 材料的位置、形式和数量。

附 件 二

敏感信息示例

II-1. 附件二为核安保相关信息安保分类方案的示例。成员国应确定准确的分类等级，以便对每一项信息进行分类。表 II-1 提供了敏感信息示例，并确定了与敏感信息相关的敏感问题。表格列出了不建议发布信息的原因并说明了安保度是否有可能会得到保障。

II-2. 表 II-1 中提供的信息类别仅表明哪些信息可能属于敏感信息。这些信息不可用作较为全面的列表或模板。根据成员国实施的专项评估考虑将相关类别纳入类似国家表格中。

II-3. 在表格中每一行的范围之内，第一列是信息示例类型。第二列说明这一类别是否通常适用于核材料和核设施（N）、其他放射性物质和相关设施（R），或两者都适用（N、R）。第三列说明这些信息可能会被视为敏感信息还是非敏感信息。最后一列对信息的敏感性和保护信息的理由做了相关解释。

II-4. 将信息指定为敏感信息并指定可能采用的分类等级时，应考虑已出现在公共领域的信息，或者以前泄露过的、或者可能泄露的信息。对此类信息的分类等级进行指定和管理可能不太合乎实际。

II-5. 如果非敏感信息与其他非敏感信息结合时可用来披露敏感信息，还应考虑将该非敏感信息指定为敏感信息。

表 II-l. 核安保相关信息的国家安保分类方案

信息类别		领域	敏感性	保护原因
1. 材料和设施安保				
1.1.	法规和导则			
A.	关于使用核材料或其他放射性物质的国家安保条例	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	这类信息通常在公共领域公布。
B.	由主管部门或其他政府机构发布的对此类规定提供的导则	核材料，核设施，及其他放射性物质和相关设施	敏感信息	虽然这些导则并非全部针对敏感性信息，但这种性质的文件可能会包含标准详情、所使用设备的类型、程序和设施的安保操作。此类细节可能会对策划恶意行为的敌对方起到帮助作用。
1.2.	国家核安保政策			
A.	有关核材料或其他放射性物质的一般性政府政策	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	这类信息通常在公共领域公布。
B.	涉及特定安保主题的详细政策	核材料，核设施，及其他放射性物质和相关设施	敏感信息	这可能会提示敌对方其可能面临的种种障碍，从而计划获取更详细的信息。

表 II-l. 核安保相关信息的国家安保分类方案（续）

信息类别	领域	敏感性	保护原因
1.3. 设施安保计划	核材料，核设施，及其他放射性物质和相关设施	敏感信息	计划通常包含现场采用的安保措施的详细信息，以及现场材料存储位置的精确信息。对于核设施，该计划还包含对现场运营至关重要的其他领域的详细信息。
1.4. 安保报告			
A. 根据安保调查、检查和评估制订的报告以及其他关于现场或设施所采用的实物保护或技术安保措施的报告	核材料，核设施，及其他放射性物质和相关设施	敏感信息	查看这些报告会使敌对方了解到材料的具体位置、保护材料所采用的措施以及可能存在的评估漏洞，从而助其避免安保措施和控制措施等赞成的阻碍。
B. 描述关键特征和/或强调安保改进要求的报告，包括要害区（如果适用）	核材料，核设施，及其他放射性物质和相关设施	敏感信息	该性质的信息会对希望避开安保安排的敌对方起到帮助作用，并且可帮助其将设施定为目标。
C. 现场或设施安保调查结果，包括对敏感信息泄露和丢失调查的结果	核材料，核设施，及其他放射性物质和相关设施	敏感信息	该性质的信息会对希望避开安保安排的敌对方起到帮助作用，并且可帮助其将设施定为目标。
D. 报告列举了安保管理制度的漏洞和发生故障产生的后果	核材料，核设施，及其他放射性物质和相关设施	敏感信息	这种性质的信息对于希望避开安保安排的敌对方会起到帮助作用。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别		领域	敏感性	保护原因
1.5.	构造详情			
A.	用来储存或加工材料的地点的构造详情和位置布局，包括在任何媒介上保存的图纸或计划，会显示与预防恶意行为有关的实物保护特征	核材料，核设施，及其他放射性物质和相关设施	敏感信息	官方地图、场地图表或平面图可由场地管理部门酌情公布，但不包括建筑物详细功能、存放在场内的材料、内部安保围栏的位置以及针对建筑物采用的其他安保措施。
B.	核电厂和其他核设施要害区的构造详情	核材料和核设施	敏感信息	这种性质的信息会帮助敌对方避开安保安排的干扰，并可能有助于其瞄准目标达到破坏目的。
1.6.	保护系统			
A.	正在使用的实物保护措施的详细信息，例如警报器、监视摄像机，出入口控制器、安保人员等	核材料，核设施，及其他放射性物质和相关设施	敏感信息	
B.	入侵检测系统传感器及相关监控摄像机的类型和位置，包括电路图、主要电源的位置、电缆走线，以及该设备的维护和测试程序	核材料，核设施，及其他放射性物质和相关设施	敏感信息	任何这种性质的信息细节都有可能对想破坏设施安保系统的敌对方起到帮助作用。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
1.7. 自动化访问控制系统的详细信息，包括计算机服务器和备份服务器及其电源的位置	核材料，核设施，及其他放射性物质和相关设施	敏感信息	不应公布任何可能导致访问控制系统被外部或内部敌对方破坏的细节。
1.8. 存储：针对材料库存的发放、接收和控制的安保程序；授权密钥持有人的姓名；针对监控和防范的安排	核材料，核设施，及其他放射性物质和相关设施	敏感信息	可能会对策划恶意行为的敌对方起到帮助作用。
1.9. 显示设施位置和限制的普通地图，但不包含详细内容	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	免费提供的互联网地图应用程序清楚地显示了这些信息。
1.10. 其他实物保护相关事宜，例如中央警报站的位置、设置、损害程度和设备；二级警报站的位置；内部区域屏障的类型	核材料，核设施，及其他放射性物质和相关设施	敏感信息	任何此类信息细节都有可能对意欲破坏核设施安保系统的敌对方起到很大的帮助作用。
2. 关于材料数量和形式的信息			
2.1. 关于在各类场地和核电厂指定地点接收或保存的核材料数量、类型和形式的信息，包括乏燃料存储的确切位置	核材料和核设施	敏感信息	此类信息会对敌对方在策划攻击行为时选择目标起到帮助作用。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别		领域	敏感性	保护原因
2.2.	吞吐量 — 标称容量、实际吞吐量和国际原子能机构保障下设施吞吐量的历史数据	核材料和核设施	非敏感信息	这类高等级的信息，特别时针对核电站的信息，往往出现在公共领域。
2.3.	其他放射性物质（包括废弃物质）的国家或地方库存，包括数量、类型、形式和确切位置	其他放射性物质和相关设施	敏感信息	此类信息会被敌对方在策划攻击时用来选择目标，从而窃取放射性物质。应该考虑哪些关于这些库存的信息已经对外公布。所有此类信息可能都不属于敏感信息。风险知情流程有助于确定是否应该将某些内容指定为敏感信息。
3. 在途材料（包括场内运输）				
3.1.	关于核材料运输第一、第二和第三类的信息	核材料和核设施	敏感信息	这些信息可以帮助敌对方在策划涉及核材料运输的恶意行为时选择目标。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别		领域	敏感性	保护原因
3.2.	高安保度车辆（HSV）			
A.	高安保度车牌	核材料和核设施	敏感信息	
B.	车辆设计和构造的物理安保特征	核材料和核设施	敏感信息	高安保度车辆专用于安保运输核材料。高安保度车辆用于运载核材料。本节列出的任何类型的信息均有可能对企图偷运或破坏在途核材料的敌对方起到帮助作用。
C.	警报器的设计和功能、固定装置和特殊锁的关键设计	核材料和核设施	敏感信息	
D.	在使用的地方，进行装货车厢钥匙、备用钥匙和暗码锁设置	核材料和核设施	敏感信息	
E.	安装在高安保度车辆上的车辆跟踪系统；系统性能和通信	核材料和核设施	敏感信息	
3.3.	核材料运输集装箱			
A.	运输集装箱对各种方式攻击的抵抗力	核材料和核设施	敏感信息	对计划蓄意破坏攻击的敌对方起到帮助作用，其目的是在运输过程中释放核材料或计划盗窃材料。
B.	集装箱规格和设计数据	核材料和核设施	非敏感信息	在未确定构造详情的情况下，这类集装箱的设计信息通常可在互联网上找到。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别		领域	敏感性	保护原因
C.	有关特殊集装箱（得到特别保护的集装箱）设计的信息	核材料和核设施	敏感信息	对计划蓄意破坏攻击的敌对方起到帮助有用，其目的是在运输过程中释放核材料或计划盗窃材料。
3.4.	运输包装：有关运输包装设计的信息	核材料和核设施	敏感信息	对计划蓄意破坏攻击的敌对方起到帮助有用，其目的是在运输过程中释放核材料或计划盗窃材料。
3.5.	其他放射性物质的运输信息	其他放射性物质和相关设施	敏感信息	此类信息，尤其是涉及强大辐射源运输的信息，可能会被敌对方用来策划盗窃行为。
	4. 对安保和安全重要的 IT 系统和计算机系统			
4.1.	IT 系统存储和处理敏感信息的详情，包括用于安保目的的系统、系统架构、所采用的计算机安保措施的详情和备份媒体的位置	核材料，核设施，及其他放射性物质和相关设施	敏感信息	信息会帮助敌对方策划针对设施的恶意行为。
4.2.	出入口控制、入侵检测系统、警报监控系统、评估和监控系统以及其他安保功能和设备的详情；以及有关备份硬件和软件位置的信息	核材料，核设施，及其他放射性物质和相关设施	敏感信息	信息会帮助敌对方策划针对设施的恶意行为。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
4.3. 与安全相关的 IT 系统或计算机系统的详细信息，包括位置、功能、升级路线、电源和备份	核材料，核设施，及其他放射性物质和相关设施	敏感信息	这类系统具有控制和操作监控功能。如果泄露这些系统信息，至少会有助于敌对方破坏设施的运行，而最坏的情况是，其破坏活动可能会导致放射性物质的释放。
5. 警卫队和快反部队			
5.1. 设施警卫队			
A. 部队的全面建立和当前能力	核材料和核设施	非敏感信息	宣传部队的存在可以让公众放心，并可能起到威慑作用。
B. 在特定地点建立部队及其当前能力	核材料和核设施	敏感信息	此类信息对于试图策划入侵核现场以实施破坏或盗窃行为的敌对方会起到帮助作用，并且可能会破坏有效应对袭击的能力。
C. 现场轮班次数	核材料和核设施	敏感信息	

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
D. 警卫队可以使用的武器和其他特殊装备以及在警卫队独立现场受过训练的枪支使用者的人数	核材料和核设施	敏感信息	任何会帮助敌对方提前预估战术行动单位的应对规模及能力的信息均不得泄露。
E. 快反部队在现场的位置、能力、武器、特殊反应车辆和时间安排	核材料和核设施	敏感信息	
F. 部署计划	核材料和核设施	敏感信息	
5.2. 负责核物质运输的护卫队			
A. 护卫队的部署和能力	核材料和核设施	敏感信息	信息会对策划攻击车队的敌对方起到帮助作用。
B. 可通过使用的无线电频率与快反部队或当地警察部队进行沟通	核材料和核设施	敏感信息	
6. 核材料衡算			
6.1. 说明			
A. 材料衡算一般性原则说明	核材料和核设施	非敏感信息	这种类型的一般性原则出现在公共领域。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
B. 设计信息问卷和说明，材料平衡区（MBA）和关键测量点（KMP）的位置	核材料和核设施	敏感信息	关于核材料的这些位置和数量的详细信息会对敌对方策划恶意行为起到帮助作用。
C. 在关键测量点进行材料测量的物理和化学形式	核材料和核设施	敏感信息	
6.2. 测量值和检测数据			
A. 标准实验室技术的精度和准确度	核材料和核设施	非敏感信息	这些信息通常出现在公共领域。
B. 显示测量灵敏度的数据或在特定工厂中不明物料量（MUF）的警报限值	核材料和核设施	敏感信息	与现场实际测量或典型测量有关的精度和准确度数据，不论是总数据还是分散数据，都会被敌对方用来策划盗窃物质的行为。
6.3. 在 IT 系统中保存的核材料流动和库存数据，通过硬拷贝或任何形式的存储介质进行保存	核材料和核设施	敏感信息	信息会表明核材料的位置和运输的详细信息。
6.4. 不明物料量			
A. 现场年度不明物料量数据不会透露有关材料平衡区的信息	核材料和核设施	非敏感信息	在许多成员国，每年汇总的不明物料量数据会公布在或可公布在公共领域。
B. 材料平衡区和关键测量点的不明物料量	核材料和核设施	敏感信息	

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
C. 对特殊不明物料量进行调查的详细信息，除非得到正式批准否则不可公布	核材料和核设施	敏感信息	但是，详细的不明物料量数据或调查结果可能会
D. 不明物料量的误差极限或对不明物料量数据不确定性的其他具体指示	核材料和核设施	敏感信息 [a]	被敌对方使用，从而将某一具体的设施定为目标，因此其属于敏感信息。
7. 许可和权限处理申请信息			
7.1. 许可和权限处理申请，不包含关于安保措施的详细信息；材料的类型、形式和数量	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	此类申请的内容取决于法律和监管框架以及具体的最终用途。如果申请内容包含对敌对方有潜在用途的敏感信息，申请也应被视为敏感信息。
7.2. 许可和权限处理申请，其中包含安保措施的详细信息以及材料的类型、形式和数量	核材料，核设施，及其他放射性物质和相关设施	敏感信息	此类申请的内容取决于法律和监管框架以及具体的最终用途。如果申请内容包含对敌对方有潜在用途的敏感信息，申请也应被视为敏感信息。
8. 安全案例、工程文件和其他安全或环境信息			
8.1. 各种级别的安全案例			尽管大多数关于安全案例的信息可能会公开透明，但有关核安保的信息可能属于敏感信息。

[a] 在一些成员国，不明物料量的误差极限值不属于敏感信息。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
A. 详细的潜在危害或可用作替代品（用于评估信息公布造成的影响）的其他信息，或公布信息造成的影响的详细信息	核材料，核设施，及其他放射性物质和相关设施	敏感信息	
B. 旨在控制或保护核材料或其他放射性物质的过程、结构和保护系统的详细优缺点	核材料，核设施，及其他放射性物质和相关设施	敏感信息	包含在安全案例中的详细信息类型会被敌对方用来选择目标并策划行动。
C. 访问生产过程的详细信息，包括实物出入控制和为了便于控制和监控而将材料从过程中去除	核材料，核设施，及其他放射性物质和相关设施	敏感信息	
9. 应急和反应计划和演习			
9.1. 应急和反应			
A. 应急和反应计划的存在	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	宣传计划的存在可以让公众放心，并可能起到威慑作用。
B. 应急和应对计划的详细内容	核材料，核设施，及其他放射性物质和相关设施	敏感信息	计划中的详细信息可以指能力、限制和响应时间，因此会被敌对方用于策划蓄意攻击行为。

表 II-l　　核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
9.2. 安保应急计划，包括详细的信息	核材料，核设施，及其他放射性物质和相关设施	敏感信息	这些文件包含的信息包括现有安保措施、警察或警卫队特遣队的能力以及对安保事件可能做出的反应。
9.3. 演习			
A. 演习即将实施或已经实施	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	公布演习的存在可以让公众放心，前提是详情的公布程度不会对敌对方起到帮助作用，例如，未来演习的日期/时间/地点。
B. 包括场景在内的现场安保演习的细节，安保计划的哪些方面正在测试，是否会涉及快反部队以及演习的结果	核材料，核设施，及其他放射性物质和相关设施	敏感信息	为敌对方提供有关快反部队反应的性质、规模、能力和时间、武装快反部队的详细情况、所采用的战术性质和信号计划的信息。
C. 安全演习的详细情况	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	安全演习通常以公开、透明的方式进行。只要不透露有关安保措施的详细信息，通常可以将其视为非敏感信息。
10. 个人信息			
10.1. 个人信息			
A. 可信度检查信息	核材料，核设施，及其他放射性物质和相关设施	敏感信息	此类信息会被用来进行勒索或敲诈。大多数国家级隐私条例要求保护此类信息。
B. 个人档案中的信息	核材料，核设施，及其他放射性物质和相关设施	敏感信息	

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
11. 放射性废弃物库存清单			
11.1. 有关放射性废弃物的信息			
A. 关于库存清单的一般信息，其中不包含可被利用的信息，例如废弃物存放在特定地点的信息，或未提供位置的废弃物的总量	核材料和核设施	非敏感信息	这些信息通常出现在公共领域，未予说明对敌对方的具体用途。
B. 可被恶意行为利用的信息，或者可用以识别设施内具体建筑物以及在其中保存的材料的信息	核材料和核设施	敏感信息	这类信息会帮助敌对方在策划破坏行为时确定目标。
12. 退役			
12.1. 退役工厂计划	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	退役设施计划通常会对外公布。
12.2. 退役遗留的废弃物 [b]			
A. 储存点即将建立，及其位置	核材料，核设施，及其他放射性物质和相关设施	非敏感信息	这些信息通常出现在公共领域。

[b] 这主要是指来自设施的污染物质，而不是设施正常运行期间操作过程中释放的放射性废弃物。

表 II-l　　核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
B. 有关构造、安保措施及即将储存在新建筑物的材料的数量和类型的详细信息，用于处理和储存退役期间处理活动产生的废弃物和受污染材料	核材料，核设施，及其他放射性物质和相关设施	敏感信息	该信息会帮助敌对方在策划破坏性攻击行为时确定目标。
13. 威胁评估和安保警报信息			
13.1. 成员国、国家安保部门或其他主管部门发布的威胁评估	核材料，核设施，及其他放射性物质和相关设施	敏感信息	通常来自国家安保材料，例如国家情报信息。
13.2. 设计基准威胁的详细信息	核材料和核设施	敏感信息	通常来自国家安保材料，例如国家情报信息。
13.3. 要害区识别研究的详细信息	核材料和核设施	敏感信息	会被敌对方用来识别目标并进行攻击。
13.4. 任何安保警报状态出现的原因和对其进行的任何更改	核材料，核设施，及其他放射性物质和相关设施	敏感信息	通常来自国家安保材料，例如国家情报信息。
14. 核技术			
14.1. 有关核材料生产或加工的详细技术信息（如浓缩铀加工和后处理）	核材料和核设施	敏感信息	此类信息可能会被敌对方利用。

表 II-l. 核安保相关信息的国家安保分类方案（续）

类别	领域	敏感性	保护原因
14.2. 提交申请许可的设计或新技术（如先进反应堆技术等）	核材料和核设施	敏感信息	尽管这些技术的详细信息可能会向公众公开，但设计或技术的某些细节可能会被敌对方利用。对此类信息进行检查以确认是否为敏感信息。
14.3. 有助于拆卸设备以获取信息来源的详细信息，或者以其他方式帮助破坏安保措施的信息	其他放射性物质和相关设施	敏感信息	这些信息会对试图移动放射性物质的敌对方有帮助。
14.4. 技术设计薄弱性研究	核材料，核设施，及其他放射性物质和相关设施	敏感信息	虽然学术研究可能会公开，但任何会导致可能被敌对方利用的薄弱点暴露的详细信息均不可在未经授权情况下进行披露。
15. 历史信息			
15.1. 和当前相关的且定性为敏感的历史信息，不论该信息是否已分类	核材料，核设施，及其他放射性物质和相关设施	敏感信息	此类信息虽然年代久远，但仍然对敌对方有用。

说明：HSV — 高安保度车辆；KMP — 关键测量点；MBA — 材料平衡区；MUL — 不明物料量；N — 核材料和核设施；R — 其他放射性物质和相关设施。

附 件 三

安保意识大纲示例

III-1. 附件三为安保意识大纲的制订提供了框架和内容范例。在确定信息安保意识大纲的内容时，组织的安保管理人员应考虑此处强调的主题和方法的具体相关性，并相应地调整大纲。

安保培训

III-2. 培训大致可分为四种类型：

(a) 意识培训提高了对威胁和薄弱点的认识，以及对保护数据、信息及其处理手段的认可（计算机和信息安保意识）。

(b) 专题培训包括对所有工作人员在安保具体方面提供的课程（分类材料处理和信息安保事件程序）。

(c) 专业培训通常是针对承担特定职责的员工提供的详细技术培训，例如系统管理员、软件开发人员、网络管理员、安保警卫员、文档分类人员和解密人员等。

(d) 在风险管理、事件预防和事件响应等方面，专业安保培训通常是管理层的重点关注点，属于专家级培训。

III-3. 该大纲包含的内容会帮助提高对以下主题的认识：

(a) 国家安保基础设施概览。

(b) 有关信息安保的各个方面，及其为何对核安保至关重要。

(c) 国家分类制度。

(d) 安保原则，例如“需要知道”和“需要持有”。

(e) 目前以下各方实施的故意行为对安保造成的威胁：

(i) 间谍和技术转让方面的敌对情报部门；

(ii) 破坏组织；

(iii) 其他个人和团体，例如信息经纪人和调查记者，其未经授权要求获得敏感信息或接触核现场和设施；

(iv) 内部人员。

(f) 敌对方组织和破坏行为造成的威胁，应考虑到极端主义派别对当今世界造成的威胁。

(g) 内部丢失或泄漏敏感信息的风险和后果，可能是由于疏忽行为造成或是为了引起窘境，还有是出于政治动机故意背叛或是为了协助恐怖主义。

(h) 可能会为潜在敌对方提供帮助或增加泄密风险的行为或活动，包括：

(i) 不严谨的行为，如对安保问题的态度散漫和随意谈论；

(ii) 会吸引敌对机构注意力的无意识的行为。因此，日常活动需要采取预防措施，包括社交方式、旅行、信件和熟人。

(i) 关于局部安保事件的信息或敌对机构正在使用的新方法类型的信息，这些信息应迅速传播。

(j) 重点是需要立即报告所有可疑情况、安保程序方面出现的已知弱点或同事表现出来的不严谨行为 — 应当广泛介绍保密行事的方式。

(k) 国家法律法规的效力及其与个人的相关性，例如有关保密、反恐、安保、数据保护和信息自由等法律，以及对违法行为的制裁和惩罚。

(l) 解释安保许可的级别；如何进行信任度检查；为何在核工业和放射性工业中其地位很重要；哪些级别的出入需要特殊许可和可信度级别，及其与上述安保威胁之间的关系。

(m) 拒绝服务（例如阻止组织在需要时访问信息，包括诸如盗窃等行为）或破坏 — 违反可用性。

(n) 未经授权修改或干扰信息 — 违反完整性。

(o) 未经授权披露 — 违反保密性。

III-4. 该大纲包含的内容可为参与者提供以下主题的培训：

(a) 关于核材料和其他放射性物质和设施的信息安保。

(b) 良好的安保实践和程序包括：

(i) 正确使用分类标记；

(ii) 实物保护、人员安保和信息安保（如文件、通信和计算机）；

(iii) 将安保规则和程序应用于员工正在或将要从事的任务中的实际范例；

(iv) 怀疑或发现破坏安保时将采取的行动。

提高安保度的其他方法

III-5. 除基本的培训计划外，还可使用其他方法使员工和承包商关注安保意识信息：

(a) 国家安保部门定期发布的安保通讯。里面可能包含关于安保问题的某些热门话题和建议。

(b) 用海报提醒个人安保遭受的威胁并告知其应对威胁所必须的主要安保控制措施。这些影响往往是暂时性的，所以海报不仅要突出显示，而且还要经常改变。

(c) 使用特殊设备时，采用贴纸提醒员工承担维护安保的个人责任。

(d) 计算机系统启动（开机）阶段的安保提醒通知，用户必须在计算机完成开机或登录操作前确认读取。（系统可记录这样的确认操作，这样用户就无法否认其已经看到过通知。）

(e) 安保管理层起草的安保通知、公告和通告，以提醒工作人员遵守某些安保规则，防止其可能会安于现状等。

(f) 提高对安保违规事件的认识，并从中吸取教训。

(g) 针对安保所遭受的具体或局部威胁对个人发出警告，并提供指导来应对威胁。

(h) 提供与个人就一般安保事宜进行沟通的渠道。

(i) 定期对个人安保知识进行测试。

(j) 只要材料的性质和敏感性在网络认可的分类级别内，组织的内联网就可以成为传达或推广安保信息的宝贵工具。

术 语 表

可用性：被授权实体根据需要可访问和使用的特性。

主管部门：由成员国指定的、履行一项或多项核安保职能的政府组织或机构。

泄密：意外或故意违反信息对象的机密性、完整性或信息丧失可用性。

机密性：未经授权的个人、实体或流程不能提供或披露信息的特性。

信息对象：对组织有价值的知识或数据。

信息安保：对信息机密性、完整性和可用性的保护。

完整性：信息准确性和全面性的特性。

需要持有：允许个人实际拥有其有效开展工作所必需的信息资产所遵守的规则。

需要知道：个人、流程和系统只能获取执行其授权职能所必需的信息、能力和资产所遵守的规则。

核材料：国际原子能机构《规约》第二十条所定义的任何特殊可裂变材料或原材料。

其他放射性物质：不属于核材料的任何放射性物质。

放射性物质：根据国家法律、法规或监管机构规定，由于其放射性而需接受监管控制的物质。

敏感信息：对其未经授权泄露、修改、变更、销毁或拒绝使用即可能影响核安保的不论何种形式的信息，包括软件。

敏感信息资产：用于存储、处理、控制或传输敏感信息的任何设备或组件。例如，敏感信息资产包括控制系统、网络、信息系统和任何其他电子或物理介质。

IAEA
国 际 原 子 能 机 构

No. 26

当 地 订 购

国际原子能机构的定价出版物可从下列来源或当地主要书商处购买。
未定价出版物应直接向国际原子能机构发订单。联系方式见本列表末尾。

北美

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
电话：+1 800 462 6420 • 传真：+1 800 338 4550
电子信箱：orders@rowman.com • 网址：www.rowman.com/bernan

世界其他地区

请联系您当地的首选供应商或我们的主要经销商：

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

交易订单和查询：
电话：+44 (0) 176 760 4972 • 传真：+44 (0) 176 760 1640
电子信箱：eurospan@turpin-distribution.com

单个订单：
www.eurospanbookstore.com/iaea

欲了解更多信息：
电话：+44 (0) 207 240 0856 • 传真：+44 (0) 207 379 0609
电子信箱：info@eurospangroup.com • 网址：www.eurospangroup.com

定价和未定价出版物的订单均可直接发送至：

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
电话：+43 1 2600 22529 或 22530 • 传真：+43 1 26007 22529
电子信箱：sales.publications@iaea.org • 网址：https://www.iaea.org/zh/chu-ban-wu

核安保中保护敏感信息的安全是一项基本原则。敏感信息所指的信息未经授权披露（或修改、变更、销毁或拒绝使用）可能危害核安保，或以其他方式协助对核设施、组织或核运输实施的恶意行为。本《实施导则》对信息安保的基本概念进行了定义，可能适用于核安保，从而帮助成员国和承担核安保责任的组织制定信息安保框架。

国际原子能机构
维也纳