ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 重要数据处理安全要求

Information security technology - Security requirements for processing of key data

（征求意见稿）

（本稿完成时间：2023 年 8 月 10 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国科学技术大学、国家信息中心、中国电子技术标准化研究院、国家信息技术安全研究中心、中国网络安全审查技术与认证中心、国家工业信息安全发展研究中心、中国信息安全测评中心、国家计算机网络应急技术处理协调中心、清华大学、中科院软件所等。

本文件主要起草人：俞能海、左晓栋、吴梦婷、李斌、许涛、陈月华、王佳慧、陈发强、胡影、周晨炜、张敏、杨晨、晏敏、杨韬、刘曦泽、陈世翔、段静辉、杨帅锋、孙岩、柳彩云、都婧、杨光、王文磊等。

信息安全技术 重要数据处理安全要求

1 范围

本文件规定了数据处理者处理重要数据的安全要求。

本文件适用于数据处理者对重要数据开展处理活动，也可供监管部门、评估机构或其他有关组织对重要数据处理活动实施安全监管、评估等活动时参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T AAAAA—2023 信息安全技术 数据分类分级规则

3 术语和定义

GB/T 25069—2022 中界定的以及下列术语和定义适用于本文件。

3.1

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。

[来源：GB/T AAAAA—2023，3.1]

3.2

数据处理 data processing

数据收集、存储、使用、加工、传输、提供、公开、删除等活动的总称。

注：也称“数据处理活动”。

3.3

数据处理者 data processor

在数据处理活动中自主决定处理目的、处理方式的组织和个人。

3.4

委托处理 entrust processing

数据处理者委托第三方按照约定的目的和方式开展的数据处理活动。

4 设施安全

4.1 系统安全

处理重要数据的系统应符合GB/T 22239—2019第三级安全要求，并通过网络安全等级保护三级（含）以上测评。

4.2 云计算服务平台安全

使用社会化云计算服务平台处理重要数据前应进行风险评估，论证重要数据上云的必要性，并重点评估云计算服务提供者的安全可信性，以及云计算服务平台的安全状况。已使用社会化云计算服务平台处理重要数据的，应定期对云计算服务平台进行安全评估。数据处理者认为云计算服务平台安全存在不可接受的安全风险时，应停止使用其处理重要数据。

5 数据处理活动的安全

5.1 收集

5.1.1 数据来源

数据处理者应：

a）制定数据收集程序，明确数据收集目的、规模、方式、范围、类型、存储期限、存储地点等，以及数据格式、质量准则和评价方式等要求；

b）在收集前进行安全评估，评估内容包括收集数据的目的、范围、频度、方式、存储期限等是否符合法律法规的规定；

c）采取合法、正当的方式收集数据；

d）验证数据的真实性、准确性，并定期对数据质量进行分析和监控，及时对异常数据进行告警、修正等；

e）跟踪和记录数据收集过程，保证数据收集活动的可追溯性。

5.1.2 数据分类制度

数据处理者应：

a）根据国家和行业主管监管部门有关数据分类的规定，和GB/T AAAAA—2023的要求，制定并定期更新本组织的数据分类管理制度；

b）结合本组织具体情况，充分考虑数据特征、业务类型等因素，在不违反国家和行业规定的前提下，可在本组织的数据分类管理制度中建立对数据进行进一步分类的规则；

c）落实本组织的数据分类制度，对本组织处理的数据进行分类。

5.1.3 数据分级制度

数据处理者应：

a）根据国家和行业主管监管部门有关数据分级的规定，和GB/T AAAAA—2023的要求，制定并定期更新本组织的数据分级管理制度；

b）结合本组织具体情况，充分考虑数据的重要程度和可能造成的危害程度，在不违反国家和行业规定的前提下，可在本组织的数据分级管理制度中，建立对数据进行进一步分级的规则，并根据安全风险变化对数据分级规则进行动态调整和优化。

5.1.4 识别重要数据

数据处理者应：

a）根据国家和行业主管监管部门有关重要数据识别的规定，和GB/T AAAAA—2023的要求，制定并定期更新本组织的重要数据识别制度；

b）根据行业特点、业务类型等因素，明确本组织重要数据的特征；

c）落实本组织的数据分级制度和重要数据识别制度，对本组织处理的数据进行分级，并识别其中的重要数据；

d）制定重要数据清单管理程序，明确清单的编制、审核、维护、更新等要求；

e）以清单方式对识别出的重要数据进行记录，标明重要数据的来源、用途、重要性时限、存储位置、存储期限、数据处理者、数据安全负责人、数据格式、数据量、访问控制规则等信息；

f）采用技术工具和措施，通过自动识别本组织重要数据的特征、自动管理重要数据清单等方法，提高对重要数据的识别效率。

5.1.5 数据目录

数据处理者应：

a）采用技术工具和措施，根据国家和行业主管监管部门有关重要数据目录的规定，对重要数据进行编目，形成重要数据目录，按规定上报国家有关部门，并定期更新维护；

b）在重要数据目录中描述数据基本情况、责任主体情况、数据处理情况、数据安全情况等信息：

1）数据基本情况，包括数据类别、数据级别、数据载体、数据来源、数据数量，以及数据详细描述等；

2）责任主体情况，包括处理者、主要负责人、数据安全负责人等；

3）数据处理情况，包括使用或共享范围和方式、是否出境、是否跨主体流动等；

4）数据安全情况，包括数据安全风险评估机构、所依据的数据分类分级标准规范、评估时间、评估结论、整改措施等。

c）定期评审和更新重要数据目录，确保目录的准确、有效、合法。

5.2 存储

5.2.1 存储保护

数据处理者应：

a）制定重要数据存储管理制度，对安全保护制度、访问流程、介质管理等作出规定；

b）落实重要数据安全管理和技术措施，并定期进行评估：

1）采用密码技术对重要数据进行保密性和完整性保护；

2）在公共信息网络与存储系统之间提供逻辑隔离措施；

3）对重要数据所在的数据中心的运维人员建立严格管理制度，对所有运维人员进行安全背景审查。

5.2.2 存储位置

数据处理者应：

a）在中国境内存储境内收集和产生的重要数据，存储重要数据的数据中心、云平台等不应设置在境外；
b）采取技术和管理措施，防止境内访问流量路由至境外；
c）对数据存储的区域进行规划，并对不同区域之间的数据流动进行安全管控。

5.2.3 存储期限

数据处理者应：
a）在重要数据清单中记录的重要性时限和存储期限到期前，以自动化方式提示数据处理者；
b）在重要性时限到期前，及时对相关数据采取转移、解密等操作，根据情况调整相关数据的保护措施；
c）采取相关技术工具和措施，及时销毁已超过存储期限或既定处理目的已不需要的重要数据。

5.2.4 备份与恢复

数据处理者应：
a）制定重要数据备份与恢复计划，明确备份与恢复的范围、频率、工具、过程、日志记录规范、数据存储期限等；
b）采用技术工具和措施，如自动化工具、异地备份等，根据既定策略自动化执行备份与恢复相关活动，并记录数据备份与恢复过程；
c）定期评审备份数据的可用性、完整性和一致性，评估数据恢复质量并采取处理措施；
d）建立数据备份与恢复技术团队，并根据数据恢复需求和目的开展数据恢复实战演练。

5.3 使用与加工

5.3.1 访问控制

数据处理者应：
a）对重要数据制定并实施访问控制策略和制度，遵循最小特权、职责分离等原则，实施安全保护措施；
b）建立统一的身份和访问管理平台，采取多因子认证、口令管理等技术措施，提供和实施对重要数据的细粒度访问控制机制，限定用户可访问数据范围，防止数据非授权的泄露、篡改和损坏；
c）严格限定重要数据所在系统的特权账号的设置和使用，及时注销弃用的账号；
d）采用相关技术，控制重要数据的使用目的和范围，降低数据泄露风险。

5.3.2 评估与审批

数据处理者应：
a）制定重要数据使用或加工前安全评估制度，明确评估要点、评估流程、审批流程等；
b）在使用或加工重要数据前进行评估，包括但不限于评估以下方面：
1）使用或加工重要数据的目的、范围、方式等是否与清单中的记录相一致，不一致的应说明理由；
2）使用或加工重要数据的人员是否符合重要数据的访问控制规则；
3）使用或加工重要数据过程中安全防护措施是否有效；
4）如重要数据使用或加工过程可能会导致数据跨主体流动，按5.4节的要求对数据接收方进一步评估；
c）由本组织数据安全负责人对评估结果进行审批，并将评估和审批记录留存3年以上。

5.3.3 保密审查

数据处理者应：

a）建立保密审查制度，明确数据保密审查的责任领导、责任部门，规定保密审查的具体责任，防止因数据汇聚等泄露国家秘密信息；

b）按照国家有关规定对数据加工结果进行保密审查，确保以预期目的、范围、方式等使用和加工重要数据；

c）建立保密审查责任追究制度，明确违规责任和处理原则；

d）在数据加工结果中发现国家秘密信息时，按国家有关保密管理规定和技术规范进行处理。

5.4 传输与提供

5.4.1 法律文件

因对外提供和共享重要数据，导致数据跨主体流动的，重要数据处理者应与数据接收方签订合同等法律文件，约定处理重要数据的目的、范围、处理方式、安全保护义务等，并约定对接收方履行安全保护义务的情况进行监督。

5.4.2 评估与审批

对外提供和共享重要数据前，数据处理者应：

a）评估以下内容：

1）数据使用目的、范围、方式，以及数据量等，确保合法、正当、必要；

2）提供和共享数据过程中数据被篡改、破坏、泄露、丢失或者被非法获取、非法利用的风险，以及对国家安全、公共利益带来的风险；

3）提供和共享数据过程中安全保护技术和管理措施的有效性；

4）接收方的诚信状况、守法情况、与境外政府机构合作关系、受政府部门处罚情况，以及接收方数据处理环境安全情况、数据安全防护能力、履行数据保护责任和义务的能力；

5）合同等法律文件的内容和效力，重点是法律文件中关于数据安全的要求能否有效约束接收方履行数据安全保护义务；

b）由本组织数据安全负责人对评估结果进行审批，并将评估和审批记录留存3年以上。

5.4.3 传输保护

对外提供和共享重要数据时，数据处理者应：

a）建立安全通道，对传输通道两端进行主体身份鉴别；

b）采取加密、签名、防重放等措施，确保数据在传输过程中的保密性、完整性、不可否认性；

c）保护网络边界安全，在不同网络区域或者安全域之间进行安全隔离；

d）提供密钥管理系统，管理密钥生成、存储、使用、分发、更新和销毁等；

e）对接收方履行安全保护义务的情况进行监督。

5.4.4 交易

将重要数据或其加工结果进行交易时，数据处理者除满足5.4.1、5.4.2、5.4.3要求外，还应：

a）验证接收方身份，管控数据交易和共享过程，防止数据被未授权使用；

b）对数据交易的全过程进行审计，并采用标记、数字水印、区块链等技术，建立对数据交易过程进行追溯的能力。

5.4.5 接收方义务

数据接收方应：

a）履行合同等法律文件规定的义务，不超出约定的目的、范围、方式处理重要数据；

b）提供不低于数据处理者的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面；

c）提供数据销毁机制，超过约定期限后对接收的重要数据进行销毁。

5.4.6 向境外提供

向境外提供重要数据时，数据处理者应按照国家规定履行以下义务：

a）向国家网信部门申报并通过数据出境安全评估；

b）采取技术和管理措施，在既定目的、范围、方式和数据类型、规模等之内进行数据跨境传输，不超出向国家申报数据出境安全评估时明确的事项等向境外提供重要数据；

c）接受和处理数据出境所涉及的用户投诉；

d）存留相关数据出境日志记录3年以上；

e）主管部门或执法部门核验向境外提供重要数据的类型、范围时，以明文、可读方式予以展示；

f）主管部门认定不应出境的，应停止数据出境，并采取有效措施对已出境数据的安全予以补救；

g）非经主管部门批准，不应向外国司法或者执法机构提供存储于中国境内的重要数据。

5.4.7 委托处理

委托处理重要数据时，数据处理者应：

a）制定委托处理管理制度，明确委托处理流程、管理要求等；

b）通过合同等法律文件，约定委托处理数据的范围和受委托处理者的数据安全保护义务；

c）采取管理和技术措施，保护委托处理过程中的数据安全；

d）监督受委托方履行数据安全保护义务的情况；

e）监督受委托方及时有效销毁已委托处理完成的数据。

5.5 公开

公开重要数据及其加工结果时，数据处理者应：

a）制定重要数据公开管理制度，明确管理和技术措施等相关要求；

b）评估公开的内容、形式、范围、期限是否合法、正当、必要，以及安全防护和管理措施的有效性；

c）定期更新和评估已公开的重要数据，对不适宜继续公开或超出公开期限的数据进行召回或销毁处理。

5.6 删除

5.6.1 数据删除

数据处理者应：

a）制定数据删除操作规范，严格按照操作规范开展重要数据的删除活动；

b）建立重要数据删除评估与审批程序，对拟删除的重要数据范围、删除理由、再利用的可能性等进行评估，经本组织数据安全负责人批准后实施数据删除；

c）提供数据删除技术措施和工具，对批准后的重要数据及其副本进行删除，包括数据处理过程中备份数据、衍生数据及操作日志数据等，确保删除后的数据以商业手段不可恢复，

d）建立数据删除效果评估机制，定期检查删除措施的有效性；

e）对数据删除过程留存日志，记录数据删除的审批、实施过程，以及被删除数据的具体情况；

f）在删除数据后及时更新重要数据清单和目录。

5.6.2 介质销毁

数据处理者应：

a）制定重要数据专用介质管理制度，明确重要数据存储介质访问和使用管理规范；

b）对重要数据存储介质进行标记，并建立重要数据与存储介质的对应关系；

c）制定存储重要数据介质的销毁管理制度，明确介质销毁处理策略、销毁对象和流程、技术措施，以及不同介质的销毁方法和机制；

d）采用技术工具和措施进行介质管理，追踪存储介质的使用和传递过程，对介质访问和使用、销毁全过程等行为进行记录和审计，并定期对销毁记录及介质销毁效果进行检查。

6 运行与管理安全

6.1 组织与人员

6.1.1 安全负责人

数据处理者应：

a）在数据处理者决策层成员中，委任重要数据安全负责人，履行重要数据安全管理职责，包括组织制定重要数据安全保护计划、组织开展风险评估等；

b）选派具备数据安全专业知识和相关管理经验的人员承担数据安全部门负责人，负责落实本组织的重要数据安全保护计划；

c）为数据安全部门负责人提供资源保障，保证其独立履行职责，并赋予其直接向网信部门和有关主管部门反映数据安全情况的权利；

d）定期（最长不超过十二个月）或在数据安全部门负责人变更时，对其能力进行评价，并根据评价结果采取培训、调岗或重新招聘等必要措施。

6.1.2 安全管理机构

数据处理者应：

a）成立数据安全管理机构，履行以下重要数据安全管理职责：

1）研究提出重要数据安全相关重大决策建议；

2）制定实施重要数据安全管理制度、操作规程和重要数据安全事件应急预案；

3）定期开展重要数据安全风险监测、风险评估、应急演练、安全宣传教育培训等活动，及时处置数据安全风险和事件；

4）按照规定及时向网信部门和主管部门报告数据安全情况；

5）掌握国家网信部门或者有关主管部门规定的特定种类、规模的重要数据的，数据安全管理机构应独立设立；

b）设立数据安全管理和技术岗位，定义岗位职责，提供人员、设备等资源；

c）明确数据管理授权审批事项、审批流程、审批部门和审批人等。

6.1.3 机构变化

重要数据处理者在发生兼并、重组、破产时，数据接收方应继续履行相关数据安全保护义务。没有数据接收方的，则以收集数据时与相关方签署的合同中约定的形式返还、删除接收数据及其加工结果。

6.1.4 管理制度

数据处理者应：

a）确保重要数据安全管理制度覆盖全部重要数据处理活动，内容包括重要数据处理目的、范围、方式、岗位、责任、管理层承诺、内外部协调及合规性要求等；

b）建立重要数据安全风险评估体系，明确安全评估周期、内容、结果使用，以及风险处置等实施细则；

c）建立重要数据安全事件投诉、举报渠道及受理处置流程，公布接受投诉、举报的联系方式、责任人等受理处置信息，及时接受、受理、处置与数据安全保护有关的投诉、举报，并依法采取停止处理、消除影响等处置措施，将处理结果告知投诉、举报人；

d）在组织架构发生重大调整或业务发生重大变化时，及时评估和修订数据安全管理制度和安全策略；

e）通过正式、有效的方式发布重要数据管理制度，确保相关职能部门、岗位和人员知悉。

6.1.5 人员

数据处理者应：

a）制定重要数据处理人员管理安全制度，明确人员招聘、录用、培训、上岗、调岗、离岗、考核、选拔等安全管理要求；

b）针对数据安全管理机构负责人和关键岗位人员，在录用前进行安全背景审查；

c）定期对重要数据处理人员进行评估和考核，依据评估、考核结果确定任职资格；

d）与重要数据处理人员签订安全责任协议，人员调离时应收回组织的软硬件资产，移交调离人员的重要数据处理岗位职责，并及时终止调离人员的重要数据处理权限；

e）重要数据处理人员调离时，与其签订保密协议，确保其调离后在合理期限内继续履行保密义务。

6.1.6 培训

数据处理者应：

a）制定年度数据安全培训计划，明确培训内容、培训时间及培训人员，培训内容包括但不限于重要数据安全管理相关法律法规、政策标准、技术实践、安全意识等；

b）根据培训计划，每年开展培训，并对培训结果进行考核、评价、记录和归档；

c）根据实际情况及时调整或定期更新培训计划。

6.2 数据治理设施

6.2.1 治理工具

数据处理者应部署数据治理工具，对重要数据开展以下活动：

a）部署和实施数据安全治理策略，落实法律法规相关的数据安全保护责任；

b）管理、监测和审计数据资产分布、使用、流转等，实现自动化数据处理与执行跟踪、合规审核和违规行为追溯；

c）评估、预测和识别潜在数据安全风险，及时采取删除、隔离、修复、减缓等补救措施；

d）建立数据处理活动的监测规则和安全基线，能根据预定义阈值对异常数据处理活动进行告警，并展示数据处理活动发生的位置、操作以及数据处理活动的风险及威胁等信息。

6.2.2 统一管理

数据处理者应通过数据治理工具实施以下措施：

a）制定和实施本组织范围内的访问控制策略，遵循最小权限和职责分离原则，实施统一的权限申请和授权管理；
b）针对有权访问重要数据的人员，统一管理账号分配，统一实施身份鉴别；
c）使用密钥管理系统，管理密钥的生成、存储、分发、使用、更新、撤销、备份、恢复、销毁和审计等；
d）使用证书管理系统，管理证书的申请、签发、发布、安装、使用、更新、吊销、归档等。

6.3 供应链管理

6.3.1 采购管理

针对处理重要数据的系统，以及数据服务，数据处理者应：
a）制定产品和服务采购策略，确保拟采购产品符合使用需求；
b）优先采购安全可信的网络产品和服务；
c）使用资产跟踪机制，如数字签名等措施，确保产品和服务生产、运输、存储、交付的安全。

6.3.2 供应商管理

针对处理重要数据的系统，以及数据服务，数据处理者应：
a）制定供应商安全管理制度，规定供应商管理目标、原则和范围，明确供应商责任和义务、与供应商合作协议的相关要求、以及内部审核原则等；
b）与供应商签署合作协议，明确双方的数据安全责任和义务，约定数据处理目的、范围、处理方式，以及保密约定和安全保护措施等；
c）监测因采购活动而导致的重要数据向供应商转移情况，确需转移的，应满足本文件关于数据提供和共享的要求，业务合作结束后应采取有效管理和技术措施督促供应商删除转移的重要数据；
d）建立信息共享机制、黑名单机制，确保供应链数据完整、可靠和安全。

6.3.3 评估

针对处理重要数据的系统，以及数据服务，数据处理者应：
a）制定和实施供应链安全评估制度，明确评估时机、内容、结果使用、风险处置等事项；
b）定期评估和审查供应链安全风险，并将评估结果应用于产品和服务采购、供应商选择和审核等过程中。

6.4 应急响应

数据处理者应：
a）制定重要数据安全事件应急预案，包括应急组织机构与职责、数据安全事件分类分级、监测与预警、应急处置流程、保障措施等事项；
b）制定并修订重要数据安全事件应急预案演练计划，定期实施应急演练，保存演练记录和演练总结报告，根据数据处理系统自身或外界环境发生重大变化时，对应急预案进行及时更新，保留审核发布记录；
c）建立应急响应中心和团队，为其配备相应的资源和技术手段；
d）建立与主管部门的数据安全事件应急处理协调沟通渠道；
e）采取技术手段监测数据安全事件并及时预警；
f）发生重要数据泄露、毁损、丢失等数据安全事件时：
1）及时启动应急处置机制，采取措施防止危害扩大，消除安全隐患；

2）及时向设区的市级网信部门和有关主管部门报告事件情况，包括涉及的重要数据数量、类型、可能的影响、已经或者拟采取的处置措施等；
3）在事件处置完毕后5个工作日内向设区的市级网信部门和有关主管部门报告事件原因、危害后果、责任处理、改进措施等情况；
4）发生特别重大的重要数据安全事件，或发现特别重大的重要数据安全威胁时，及时向国家网信部门、国务院公安部门和有关主管部门报告。

6.5 审计

数据处理者应：

a）制定审计策略，对重要数据处理活动进行审计，满足数据安全事件处置、应急响应、责任追究等需要；
b）记录重要数据访问权限变动、数据重要性变动、数据分类分级变动等情况；
c）记录数据加工前后的数据变化情况，包括标识数据源和跟踪数据处理过程，能准确还原各加工阶段的数据状态，支撑对异常数据来源、数据状态关联等的审查；
d）采取技术措施和工具，保护审计记录的完整、准确、不可否认和正确使用。

6.6 风险评估

数据处理者应：

a）建立数据安全风险评估制度，明确数据安全风险评估流程、评估内容、评估时机等；
b）至少在以下情况进行重要数据安全评估，并编制、留存风险评估报告：
1）开展重要数据共享、交易、委托处理、向境外提供等活动之前；
2）法律法规有新的要求时；
3）业务模式、信息系统、运行环境发生重大变更时；
4）发生重要数据安全事件时；
c）每年对重要数据处理活动开展评估，并向设区的市级网信部门和有关主管部门报送风险评估报告，内容包括但不限于：
1）重要数据处理者基本信息、重要数据安全管理机构信息、重要数据安全负责人信息；
2）本年度处理重要数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括重要数据内容本身；
3）重要数据安全管理制度及实施情况，重要数据备份、加密、访问控制等安全保护措施及有效性；
4）发现的重要数据安全风险，发生的重要数据安全事件及处置情况；
5）提供、共享、委托处理重要数据的风险评估情况；
6）重要数据出境情况，包括数据接收方名称、联系方式、出境数据的类型、数量及目的，重要数据在境外的存储地点、存储期限、适用范围和方式等。

6.7 配合监督管理

数据处理者应：

a）制定配合主管部门或执法部门进行重要数据安全监督检查的流程和规范，明确自身权益保障要求、配合义务等事项；
b）在符合法律程序的条件下，开放数据访问、提供技术支持等，解释说明组织运作、技术系统、算法原理、数据处理程序等；

c）在有关部门发现重要数据处理活动存在较大安全风险时，根据要求采取暂停用户注册、修改算法等防止风险扩大的而措施。

参考文献

[1] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[2] NIST SP 800-172A Assessing Enhanced Security Requirements for Controlled Unclassified Information