Holland & Knight
美国霍兰德奈特律师事务所
www.hklaw.com

CHINA PRACTICE 期刊
NEWSLETTER

January - February 2023
2023 年 1、2 月刊

Table of Contents

China Practice Newsletter

Holland & Knight is a U.S.-based global law firm committed to provide high-quality legal services to our clients. We provide legal assistance to Chinese investors and companies doing business or making investments in the United States and Latin America. We also advise and assist multinational corporations and financial institutions, trade associations, private investors and other clients in their China-related activities. With more than 1,700 professionals in 32 offices, our lawyers and professionals are experienced in all of the interdisciplinary areas necessary to guide clients through the opportunities and challenges that arise throughout the business or investment life cycles.

We assist Chinese clients and multinational clients in their China-related activities in areas such as international business, mergers and acquisitions, technology, oil and energy, healthcare, real estate, environmental law, private equity, venture capital, financial services, taxation, intellectual property, private wealth services, data privacy and cybersecurity, labor and employment, ESOPs, regulatory and government affairs, and dispute resolutions.

We invite you to read our China Practice Newsletter, in which our authors discuss pertinent Sino-American topics. We also welcome you to discuss your thoughts on this issue with our authors listed within the document.

霍兰德奈特律师事务所是一家位于美国的全球性法律事务所，我们致力于向客户提供高质量的法律服务。我们向在美国及拉丁美洲进行商业活动或投资的中国投资人及公司提供他们所需的各类法律协助。我们也向跨国公司、金融机构、贸易机构、投资人及其他客户提供他们于其与中国相关活动中所需的咨询和协助。我们在 32 个办公室的 1700 多名对各领域有经验的律师及专业人员能够协助客户处理他们在经营或投资过程中所遇到的各种机会及挑战。

我们向中国客户及从事与中国有关活动的跨国客户提供法律协助的领域包括国际商业、企业并购、科技法律、石油及能源、医疗法律、房地产、环保法律、私募基金、创投基金、金融法律服务、税务、知识产权、私人财富管理法律服务、信息隐私及网络安全、劳动及雇佣法律、员工持股计划、法令遵循及政府法规、及争议解决。

我们邀请您阅读刊载我们各作者就与中美有关的各议题所作论述的 China Practice 期刊。我们也欢迎您向本期刊的各作者提供您对各相关议题的看法。

Commerce Department Rolls Out Measures to Strengthen Export Controls on China

ACTION TARGETS ADVANCED COMPUTING, SEMICONDUCTOR MANUFACTURING ITEMS, AND SUPERCOMPUTER AND SEMICONDUCTOR END USES

By Andrew K. McAllister, Robert A. Friedman, Sulan He and Sergio A. Fontanez

HIGHLIGHTS:

- The U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued an interim final rule on Oct. 7, 2022, placing unilateral export controls against China on certain advanced computing items and semiconductor manufacturing items.
- All U.S. and non-U.S. businesses with a connection to China, especially those in the emerging technology sector, should closely review the above items as well as items that support the semiconductors and supercomputers industries.
- The new rule was effective in phases over the course of October 2022, and public comments closed in mid-December 2022.

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued an interim final rule on Oct. 7, 2022, placing unilateral export controls on certain advanced computing items and semiconductor manufacturing items. The interim final rule is aimed at restricting China's ability to obtain advanced computing chips, develop and maintain supercomputers and manufacture advanced semiconductors.

The new rule aligns with the recent executive order mandating the Committee on Foreign Investment in the United States (CFIUS) to consider the effect of foreign investments on U.S. technological leadership in microelectronics, artificial intelligence (AI) and quantum computing. (See previous Holland & Knight alert, "New Executive Order Creates Roadmap of Heightened CFIUS Scrutiny for Cross-Border M&A," Sept. 20, 2022.) This new rule follows a trend by the Biden Administration to maintain U.S. technological leadership in these areas.

The rule makes the following key changes:

NEW EXPORT CONTROL CLASSIFICATION NUMBERS AND LICENSE REQUIREMENTS

BIS has imposed Regional Stability (RS) controls and a license requirement for exports, reexports and in-country transfers of identified items to or within China. BIS is adding new Export Control Classification Numbers (ECCNs) as noted below:

- ECCN 3A090 – certain high-performance integrated circuits (ICs)
- ECCN 3B090 – certain semiconductor manufacturing equipment and specially designed parts, components and accessories therefor

- ECCN 4A090 – computers, electronic assemblies and components containing ICs exceeding the limit in ECCN 3A090.a

- ECCN 4D090 – software specially designed or modified for the development or production of items controlled under ECCN 4A090

Additionally, BIS revises a couple of existing ECCNs – including ECCNs 3D001, 3E001 and 4E001 – to align the new RS controls for ECCNs 3A090 and 4A090 in the related "software" and "technology" ECCNs. The new RS controls are also added to the license requirement tables within ECCNs 5A992 and 5D992 to address circumstances when these ECCNs meet or exceed the performance parameters of ECCNs 3A090 and 4A090.

Importantly, the new license requirements do not apply to so-called "deemed" exports or "deemed" reexports. Therefore, a license is not required for the release or disclosure of controlled technology to Chinese persons located outside of China.

To minimize the short-term impact on the semiconductor supply industry for items that are ultimately destined to customers outside of China, the rule establishes a Temporary General License (TGL), effective until April 7, 2023, that permits exports, reexports, transfers (in-country) and exports from abroad for items subject to the additional licensing requirements when destined to or within China by companies not headquartered in Country Groups D:1, D:5 or E for specific activities. The TGL applies to "items covered by ECCNs 3A090, 4A090, and associated software and technology in ECCN 3D001, 3E001, 4D090, or 4E001."

NEW VARIANTS OF THE FOREIGN DIRECT PRODUCT (FDP) RULE

The foreign direct product (FDP) rule is intended to capture items manufactured outside of the United States that are produced using certain U.S. technology.

Entity List FDP Rule

BIS expands its FDP rule to apply to 28 China-based entities that were already on the Entity List. Specifically, non-U.S. exporters will require a license to export, reexport or transfer a foreign-produced item that is either:

- a "direct product" of "technology" or "software" classified as ECCNs: 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D993, 4D994, 4E001, 4E992, 4E993, 5D001, 5D002, 5D991, 5E001, 5E002 or 5E991

- produced by any plant or "major component" of a plant when the plant or "major component" of a plant itself is a "direct product" of U.S.-origin "technology" or "software" specified in the ECCNs above.

Advanced Computing FDP Rule

The Advanced Computing FDP Rule applies if the individual or entity has "knowledge" that the foreign-produced item is: 1) destined for China or will be incorporated into any "part," "component," "computer" or "equipment" not designated EAR99 that is destined to China or 2) technology developed by an entity headquartered in China for the "production" of a mask or an IC wafer or die. Further, the foreign-produced item must be either:

- the "direct product" of "technology" or "software" subject to the EAR and specified in 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D090, 4D993, 4D994, 4E001, 4E992, 4E993, 5D001, 5D002, 5D991, 5E001, 5E991 or 5E002 and

- the foreign-produced item is specified in ECCN 3A090, 3E001 (for 3A090), 4A090 or 4E001 (for 4A090) or

- the foreign-produced item is an IC, computer, "electronic assembly" or "component" specified elsewhere on the Commerce Control List (CCL) and meets the performance parameters of ECCN 3A090 or 4A090

- produced by any plant or "major component" of a plant that is located outside the United States, when the plant or "major component" of a plant, whether made in the United States or a foreign country, itself is a "direct product" of U.S.-origin "technology" or "software" that meets the requirements discussed immediately above.

"Supercomputer" FDP Rule

The Supercomputer FDP rule expands the scope of the Export Administration Regulations (EAR) to certain items destined for China whenever the exporter has "knowledge" that the foreign-produced item will be 1) used in the design, "development," "production," operation, installation (including on-site installation), maintenance (checking), repair, overhaul or refurbishing of a "supercomputer" (as defined in the EAR) located in or destined to China or 2) incorporated into or used in the "development" or "production" of any "part," "component" or "equipment" that will be used in a "supercomputer" located in or destined to China. Further, the foreign-produced item must be either:

1. the "direct product" of "technology" or "software" subject to the EAR and specified in ECCNs 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D993, 4D994, 4E001, 4E992, 4E993, 5D001, 5D991, 5E001, 5E991, 5D002 or 5E002

2. produced by any plant or "major component" of a plant that is located outside the United States, when the plant or "major component" of a plant, whether made in the United States or a foreign country, itself is a "direct product" of U.S.-origin "technology" or "software" that is specified in the ECCNs 3D001, 3D991, 3E001, 3E002, 3E003, 3E991, 4D001, 4D994, 4E001, 4E992, 4E993, 5D001, 5D991, 5E001, 5E991, 5D002 or 5E002.

"Supercomputers" is defined as "A computing 'system' having a collective maximum theoretical computer capacity of 1090 or more double-precision (64-bit) petaflop or 200 or more single-precision (32-bit) petaflops within a 41600 cubic feet or smaller envelope."

END-USER/END-USE CONTROLS

Additionally, the new rules impose end-user and end-use controls based upon an individual or entity's knowledge that certain items subject to the EAR are destined for a supercomputer or semiconductor development or production end-use in China. These prohibitions include:

1. any item subject to the EAR from being used in the "development" or "production" of ICs at a semiconductor fabrication "facility" located in China that fabricates certain ICs such as advanced logic, NAND and DRAM ICs;

2. any item subject to the EAR when such items will be used for the "development," "production," "use," "operation," installation (including on-site installation), maintenance (checking), repair, overhaul or refurbishing of a "supercomputer" located in or destined to China; and

3. any item subject to the EAR that will be used in the "development" or "production" in China of any "parts," "components" or "equipment" specified under ECCNs 3B001, 3B002, 3B090, 3B611, 3B991 or 3B992.

U.S. PERSON ACTIVITIES

In a broad expansion with sanctions-like restrictions, U.S. persons are prohibited from engaging in certain activities, even when the items are not subject to the EAR (e.g., non-U.S. origin items). Accordingly, BIS will require a U.S. person to obtain a license to engage in (or facilitate) shipping, transmitting, transferring or servicing:

- items not subject to the EAR that the individual or company knows will be used in the "development" or "production" of ICs at a semiconductor fabrication "facility" located in China that fabricates certain ICs, including advanced logic ICs, NAND memory ICs or DRAM ICs;
- items not subject to the EAR and meeting the parameters of any ECCN in Product Groups B, C, D or E in Category 3 of the CCL that the individual or company knows will be used in the "development" or "production" of integrated circuits at any semiconductor fabrication "facility" located in China, for which the individual or company does not know whether such semiconductor fabrication "facility" fabricates certain ICs, including advanced logic ICs, NAND memory ICs or DRAM ICs; and
- items not subject to the EAR but meeting the parameters of ECCN 3B090, 3D001 (for 3B090) or 3E001 (for 3B090) regardless of end use or end user.

PUBLIC BRIEFING

During the public briefing held in conjunction with the issuance this rule, BIS noted that, while some terms may be undefined, it would not define additional terms during the comment period, which closed in mid-December 2022. However, BIS will provide frequently asked questions and answers on a rolling basis.

CONSIDERATIONS

In light of these new rules, it would be prudent for companies to engage in proactive steps which may include:

- export classification – confirm appropriate classification for ICs and semiconductor manufacturing equipment (and related parts, components and accessories);
- enhanced diligence – review and bolster internal procedures meant to identify end use in China, particularly as it relates to supercomputers or semiconductor development or production; and
- third-country activities – assess manufacturing activities outside of the United States to determine whether any items being shipped to China tie to advance computing or supercomputers.

If you would like guidance in evaluating how novel export controls, including how these new rules may affect your business, please contact the authors or another member of Holland & Knight's International Trade Group.

商务部出台加强对中国出口管制的措施

行动针对高级计算、半导体制造产品、以及超级计算机和半导体最终用途

原文作者：Andrew K. McAllister 、Robert A. Friedman 、Sulan He 及 Sergio A. Fontanez

重点摘要:

- 美国商务部工业与安全局（BIS）于 2022 年 10 月 7 日发布了一项暂行最终规则，就某些先进计算机产品和半导体制造产品对中国实施单边出口管制。
- 所有与中国有联系的美国和非美国企业，尤其是新兴技术领域的企业，都应仔细审查上述项目以及支持半导体和超级计算机行业的项目。
- 新规定于 2022 年 10 月分阶段生效，公众意见征询于 2022 年 12 月 中旬截止。

美国商务部工业与安全局 (BIS) 于 2022 年 10 月 7 日发布了一项暂行最终规则，就某些先进计算机产品和半导体制造产品实施单边出口管制。暂行最终规定旨在限制中国获得先进计算芯片、开发和维护超级计算机以及制造先进半导体的能力。

新规则符合最近的行政命令，该命令要求美国外国投资委员会（CFIUS）考虑外国投资对美国在微电子、人工智能 (AI) 和量子计算领域技术领先地位的影响。 （请参阅之前的 Holland & Knight 提示文章，“新的行政命令制定了加强 CFIUS 对跨境并购的审查的路线图”，2022 年 9 月 20 日。）。这项新规定遵循了拜登政府为保持美国在这些领域的技术领先地位的趋势.

该规则进行了以下关键更改：

新的出口管制分类编号和许可证要求

BIS 对向中国境内或在中国境内出口、再出口和国内转移已确定物品实施了区域稳定性（RS）控制和许可要求。 BIS 正在添加新的出口管制分类编号 (ECCN)，如下所示：

- ECCN 3A090 – 某些高性能集成电路 (IC)
- ECCN 3B090 – 某些半导体制造设备及为其专门设计的零件、组件和配件
- ECCN 4A090 – 包含超过 ECCN 3A090.a 所限制的 IC 的计算机、电子组件和组件
- ECCN 4D090 – 为开发或生产受 ECCN 4A090 控制的项目而专门设计或修改的软件

此外，BIS 修订了几个现有的 ECCN——包括 ECCN 3D001、3E001 和 4E001——以在相关“软件”和“技术”ECCN 中调整 ECCN 3A090 和 4A090 的新的区域稳定性控制。新的区域稳定性控制也被添加到 ECCN 5A992 和 5D992 中的许可证要求表中，以处理这些 ECCN 达到或超过 ECCN 3A090 和 4A090 的性能参数的情况。

重要的是，新的许可证要求不适用于所谓的“视为”出口或“视为”再出口。因此，向位于中国境外的中国人士发布或披露受控技术不需要许可证。

为了将最终运往中国境外客户的物品对半导体供应行业的短期影响降至最低，该规则建立了临时通用许可证（TGL），有效期至 2023 年 4 月 7 日，允许总部不在国家组 D:1、D:5 或 E 的公司为特定活动出口、再出口、（内国）转运运往中国或在中国境内出口受额外许可要求约束的物品。 TGL 适用于“ECCN 3A090、4A090 以及 ECCN 3D001、3E001、4D090 或 4E001 中的相关软件和技术涵盖的项目”。

外国直接产品（FDP）规则的新变体

外国直接产品（FDP）规则旨在涵盖使用某些美国技术生产的在美国境外制造的物品。

实体清单 FDP 规则

BIS 将其 FDP 规则扩大到适用于实体清单上已有的 28 个中国实体。具体而言，非美国出口商将需要许可证才能出口、再出口或转让外国生产的物品，该物品是：

- 归类为以下 ECCN 的“技术”或“软件”的“直接产品”：3D001、3D991、3E001、3E002、3E003、3E991、4D001、4D993、4D994、4E001、4E992、4E993、5D001、5D002、5D9001、5D901、5D001 或 5E991
- 当工厂或工厂的“主要部件”本身是上述 ECCN 中指定的美国原产“技术”或“软件”的“直接产品”时，而由任何工厂或工厂的“主要部件”所生产的。

高级计算 FDP 规则

如果个人或实体“知道”外国生产的物品是：1）运往中国或将被纳入运往中国的不被指定为 EAR99 的任何“部件”、“组件”、“计算机”或“设备”、或 2）由总部位于中国的实体开发的用于“生产”掩模或 IC 晶圆或芯片的技术，则适用高级计算 FDP 规则。此外，外国生产的物品必须是：

- 受 EAR 约束并为在 3D001、3D991、3E001、3E002、3E003、3E991、4D001、4D090、4D993、4D994、4E001、4E992、4E993、5D001、5D002、5D002、 5D991、5E001、5E991 或 5E002 中指定的“技术”或“软件”的“直接产品”，且
    - ECCN 3A090、3E001（对于 3A090）、4A090 或 4E001（对于 4A090）所指定的外国生产物品，或
    - 外国生产的物品是商业控制清单（CCL）中其他地方指定的 IC、计算机、“电子组件”或“组件”，并且符合 ECCN 3A090 或 4A090 的性能参数

- 由位于美国境外的任何工厂或工厂的“主要部分”生产，而该工厂或工厂的“主要部件”，无论是在美国还是外国制造，本身就是符合上述要求的源自美国的“技术”或“软件”的 “直接产品”。

“超级计算机”FDP 规则

超级计算机 FDP 规则将出口管理条例（EAR）的范围扩大到某些运往中国的物品，只要出口商“知道”外国生产的物品将 1）用于设计、“开发”、“生产”， ″位于或运往中国的“超级计算机”（定义见 EAR）的操作、安装（包括现场安装）、维护（检查）、修理、检修或翻新，或 2）并入或用于“开发”或“生产”将用于位于或运往中国的“超级计算机”的任何“零件”、“组件”或“设备”。此外，外国生产的物品必须是：

1. 受 EAR 约束并在 ECCN 3D001、3D991、3E001、3E002、3E003、3E991、4D001、4D993、4D994、4E001、4E992、4E993、5D001、5D901、5E001、5E003 、 5E991、5D002 或 5E002 中指定的“技术”或“软件”的“直接产品”

2. 由位于美国境外的任何工厂或工厂的“主要部件”生产，而该工厂或工厂的“主要部件”，无论是在美国还是外国制造，本身就是 ECCN 3D001、3D991、3E001、3E002、3E003、3E991、4D001、4D994、4E001、4E992、4E993、5D001、5D991、5E001、5E002 或 5E002 中指定的源自美国的“技术”或“软件”的“直接产品”

“超级计算机”被定义为“在 41600 立方英尺或更小的封装内具有 1090 或更多双精度（64 位）千兆级浮点运算或 200 或更多单精度（32 位）千兆级浮点运算的集体最大理论计算机容量的计算’系统’。”

最终用户/最终用途控制

此外，新规则根据个人或实体的知识对最终用户和最终用途实施控制，即受 EAR 约束的某些物品将用于中国的超级计算机或半导体开发或生产最终用途。这些禁令包括：

1. 在位于中国的半导体制造“设施”中用于制造某些 IC（例如高级逻辑、NAND 和 DRAM IC）的 IC“开发”或“生产”时受 EAR 约束的任何物品；

2. 受 EAR 约束的任何项目，当这些项目将用于“开发”、“生产”、“使用”、“操作”、安装（包括现场安装）、维护（检查）、修理、大修或翻新位于或运往中国的“超级计算机”；和

3. 任何受 EAR 约束的项目，将用于在中国“开发”或“生产”ECCN 3B001、3B002、3B090、3B611、3B991 或 3B992 规定的任何“零件”、“组件”或“设备”。

美国人士活动

在具有类似制裁限制的广泛扩展中，美国人士被禁止从事某些活动，即使这些项目不受 EAR 的约束（例如，非美国原产项目）。因此，BIS 将要求美国人士获得从事（或促进）运输、传输、转移或服务的许可证：

- 个人或公司知道的不受 EAR 约束的物品将在位于中国的半导体制造“设施”用于制造某些 IC，包括高级逻辑 IC、NAND 存储器 IC 或动态随机存取存储器集成电路；

- 不受 EAR 约束且符合 CCL 第 3 类产品组 B、C、D 或 E 中任何 ECCN 参数的项目，个人或公司知道这些项目将用于集成电路的“开发”或“生产”在位于中国的任何半导体制造“设施”中，个人或公司不知道该半导体制造“设施”是否制造某些 IC，包括高级逻辑 IC、NAND 存储器 IC 或 DRAM IC；和

- 不受 EAR 约束但满足 ECCN 3B090、3D001（对于 3B090）或 3E001（对于 3B090）参数的项目，无论最终用途或最终用户如何。

公开简报

在与发布此规则同时举行的公开简报会上，BIS 指出，虽然某些术语可能未定义，但在 2022 年 12 月中旬结束的评论期内不会定义其他术语。但是，BIS 将提供滚动的常见问题和答案。

注意事项

鉴于这些新规则，公司采取积极主动的措施将是谨慎的做法，其中可能包括：

- 出口分类——确认 IC 和半导体制造设备（以及相关零件、组件和配件）的适当分类；

- 加强尽职调查——审查和加强旨在识别中国最终用途的内部程序，特别是与超级计算机或半导体开发或生产相关的程序；和

- 第三国活动——评估美国境外的制造活动，以确定运往中国的任何物品是否与高级计算或超级计算机有关。

如果您希望寻求有关评估新的出口管制的指导（包括这些新规则可能对您的业务的影响），请联系作者或 Holland & Knight 的 International Trade 业务团队。

CFIUS Enforcement and Penalty Guidelines Enhance Transparency for Cross-Border Dealmakers

By Antonia I. Tzinova, Sergio A. Fontanez and Robert A. Friedman

HIGHLIGHTS:

- The Committee on Foreign Investment in the United States (CFIUS) on Oct. 20, 2022, released enforcement and penalty guidelines that enhance transparency for cross-border dealmakers and provide the public – for the first time – important information about how CFIUS will assess whether and what penalty to impose for a violation of its regulations.
- The guidelines outline aggravating and mitigating factors that CFIUS may consider in making such a determination.

The Committee on Foreign Investment in the United States (CFIUS) released the first-ever CFIUS Enforcement and Penalty Guidelines (Guidelines) on Oct. 20, 2022, providing the public a roadmap describing three categories of conduct that may constitute a violation of the CFIUS regulations, the process the Committee generally follows in imposing penalties and some of the factors it considers in determining whether a penalty is warranted and the scope of any such penalty. These Guidelines also highlight the importance of prompt and complete self-disclosure of any conduct that may constitute a violation.

The Guidelines align with other regulatory regimes involved with protecting U.S. national security, such as export controls and economic sanctions, that incentivize voluntary self-disclosures of violations and reward parties for enhanced compliance measures, while applying less favorable treatment to repeat offenders and those that ignore or obfuscate prohibited conduct.

TYPES OF CONDUCT THAT MAY CONSTITUTE A VIOLATION OF CFIUS REGULATIONS

The Guidelines address three categories of acts or omissions that may constitute a violation:

1. **Failure to file** a mandatory declaration in a timely manner.
2. Conduct that is prohibited by or otherwise **fails to comply** with CFIUS mitigation agreements, conditions or orders (CFIUS Mitigation).
3. **Material misstatements, omissions or false certifications** in relation to any information submitted to CFIUS in connection with its review, or CFIUS Mitigation, including information "provided during informal consultations."

SOURCES OF INFORMATION ON WHICH CFIUS RELIES

The Guidelines outline the primary sources CFIUS utilizes to receive information in connection to evaluating potential violations.

- **Requests for Information:** CFIUS often requests information from individuals and entities to monitor compliance with CFIUS mitigation, investigate potential violations and determine if any enforcement action is necessary. It is important to remember that compliance with these requests for information is a positive factor when CFIUS is considering appropriate enforcement actions.

- **Self-Disclosure:** CFIUS strongly encourages any person who engaged in conduct that may constitute a violation to submit a timely self-disclosure, even if not explicitly required by any applicable CFIUS agreement, law or regulation. Self-disclosures should be in written form and provide a complete description of what may constitute a violation, including all parties involved. Timely and complete self-disclosures will also be considered positive factors when CFIUS is determining whether a penalty or other remedial measures are necessary. A key factor in "timeliness" is whether discovery of the conduct at issue by CFIUS or other government officials has already occurred or was imminent prior to the self-disclosure. CFIUS will also consider whether the reporting party or parties complied with any applicable CFIUS mitigation requiring the disclosure of the conduct. If a business is in the process of completing an internal investigation of a potential violation, it should still make an initial self-disclosure to CFIUS and follow up with a complete self-disclosure.

- **Tips:** CFIUS encourages parties to submit tips, referrals or other relevant information to the CFIUS tips line found on the CFIUS Monitoring and Enforcement Page.

PENALTY PROCESS

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) and CFIUS regulations provide the maximum penalties that may be assessed based on different violations. Specifically:

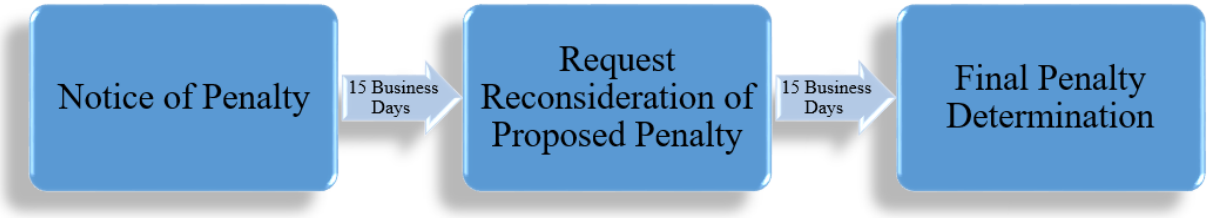
- Any person who submits a declaration or notice with a material misstatement or omission or makes a false certification under 31 Section 800.404, Section 800.405 or Section 800.502 may be liable for a civil penalty not to exceed $250,000 per violation.

- Any person who fails to comply with the requirements of Section 800.401 may be liable for a civil penalty not to exceed $250,000 or the value of the transaction, whichever is greater.

- Any person who violates, intentionally or through gross negligence, a material provision of a mitigation agreement under Section 721(l) of the Defense Production Act may be liable for a civil penalty not to exceed $250,000 per violation or the value of the transaction, whichever is greater.

In each case, the penalty is per violation, which suggests that violations can be cumulated, meaning that CFIUS might find more than one violation and assess a penalty higher than the maximum per violation. This determination shall be based on the nature of the violation.[1]

The Guidelines provide a roadmap for the penalty process as described in 31 C.F.R. Section 800.901. First, CFIUS sends a notice of penalty, including a written explanation of the conduct to be penalized and the amount of any monetary penalty to be imposed. The notice will state the legal basis for concluding that the conduct constitutes a violation and may set forth any aggravating and mitigating factors that the Committee considered. Second, the recipient may (but is not required to) submit a petition of reconsideration, within 15 business days, including any defense, justification, mitigating factors or explanation (the period may be extended by written agreement upon a showing of good cause). Finally, CFIUS will consider any petition it receives before issuing a final penalty determination within 15 business days of receipt of the petition (the period may be extended by written agreement).



Aggravating/Mitigating Factors*

- Accountability and Future Compliance
- Harm to U.S. National Security
- Negligence, Awareness, and Intent
- Persistence and Timing
- Response and Remediation
- Sophisitcation of CFIUS Compliance Program
- Record of CFIUS Compliance

*This is a non-exhaustive list

When considering a penalty for a CFIUS violation, CFIUS weighs a number of aggravating and mitigating factors in its fact-based analysis. Below, this article highlights a few of the most notable considerations for businesses (a full list is available here):

- **Accountability and Future Compliance:** the need to impose accountability for conduct and incentivize future compliance
- **Harm:** the impact of the violation on U.S. national security
- **Negligence, Awareness and Intent:** the extent to which the conduct was the result of simple negligence, gross negligence, intentional action or willfulness; any effort to conceal or delay the sharing of relevant information with CFIUS; and the seniority of personnel within the entity that knew or should have known about the conduct
- **Persistence and Timing:** the length of time that elapsed between awareness of the conduct and CFIUS reporting, along with the frequency and duration of the conduct
- **Response and Remediation:** the existence of self-disclosure, including the timeliness, nature and scope of information reported to CFIUS; whether there was complete cooperation in the CFIUS investigation; and whether there was prompt, complete and appropriate remediation of the conduct
- **Sophistication and Record of Compliance:** a business's history and familiarity with CFIUS; internal and external resources dedicated to compliance with applicable legal obligations (e.g., legal counsel, consultants, auditors and monitors); policies, training and procedures in place to prevent the conduct and the reason for the failure of such measures; the compliance culture that exists within the company; and the experience of other federal, state, local or foreign authorities with knowledge of the business in the assessment of the quality and sufficiency of compliance with applicable legal obligations

TOP 3 TAKEAWAYS

The CFIUS Process Is Extremely Complex. The penalty guidelines, in combination with a recent Executive Order on expanded factors in the CFIUS review process, provide flashing signals to the public of CFIUS heightened scrutiny of and commitment to protect industry sectors of particular importance to U.S. national security. An analysis of CFIUS jurisdiction is now a *de facto* requirement in all cross-border investments or acquisitions.

Any Communication to CFIUS May Be the Basis for a Violation. The Enforcement and Penalty Guidelines make clear that any and all submissions to CFIUS (whether in the context of assessments, reviews, investigations, mitigation or informal consultations) should be complete, transparent and done in a timely manner. CFIUS considers each of these as aggregating or mitigating factors in assessing potential penalties.

Dedicated Resources and Commitment to Compliance Are Mitigating Factors. The Enforcement and Penalty Guidelines expressly call out – as mitigating factors – businesses' internal and external resources dedicated to compliance with applicable CFIUS legal obligations (including legal counsel), along with policies, training and procedures in place to prevent prohibited conduct. These factors clearly underscore the regulatory value of having an expert conduct standard CFIUS-related due diligence for all cross-border transactions and perform a CFIUS risk assessment, as appropriate, to fully vet all CFIUS considerations.

If you have any questions about this article or seek assistance formulating a CFIUS strategy, reach out to the authors or another member of Holland & Knight's CFIUS and Industrial Security Team. Our attorneys have the knowledge and experience to conduct the necessary due diligence to identify covered transactions, prepare the necessary CFIUS risk assessments to equip business leaders with tools to evaluate regulatory risk and help navigate the evolving CFIUS landscape.

Notes

[1] See 31 Section 800.901.

CFIUS 执法和处罚准则为跨境交易投资人提高了透明度

原文作者：Antonia I. Tzinova、Sergio A. Fontanez 及 Robert A. Friedman

重点摘要:

- 美国外国投资委员会 (CFIUS) 于 2022 年 10 月 20 日发布了执法和处罚准则，为跨境交易投资人提高了透明度，并首次向公众提供有关 CFIUS 将如何评估是否及如何对违反其规定进行处罚的重要信息。
- 该准则概述了 CFIUS 在做出此类决定时可能考虑的加重和减轻因素。

美国外国投资委员会 (CFIUS) 于 2022 年 10 月 20 日发布了首个 CFIUS 执法和处罚准则（简称“准则”），为公众提供了一份路线图，描述了可能构成违反 CFIUS 的三类行为类型、CFIUS 在实施处罚时通常遵循的程序以及在决定是否有必要进行处罚以及决定任何该等处罚的范围时考虑的一些因素。这些准则还强调了及时和完整地自我披露任何可能构成违规行为的重要性。

该准则与涉及保护美国国家安全的其他监管制度（例如出口管制和经济制裁）保持一致，这些制度鼓励自愿自我披露违规行为并奖励各方加强合规措施，同时对屡犯和忽视或混淆被禁止的行为者施加较不利的待遇。

可能构成违反 CFIUS 规定的行为类型

该准则提到三类可能构成违规的行为或不作为：

1. **未能**及时**提交**强制申报。
2. 从事 CFIUS 缓解协议、条件或命令（CFIUS 缓解措施）所禁止的行为或**未能遵守** CFIUS 缓解措施。
3. 对提交给 CFIUS 的与其审查或 CFIUS 缓解措施相关的任何信息（包括“在非正式磋商期间提供的信息”）中有**重大错误陈述、遗漏或虚假证明。**

CFIUS 依赖的信息来源

该准则概述了 CFIUS 用于接收与评估潜在违规行为相关的信息的主要来源。

- **信息请求：** CFIUS 经常要求个人和实体提供信息，以监督 CFIUS 缓解措施的遵守情况、调查潜在的违规行为并确定是否有必要采取任何执法行动。重要的是要记住，在 CFIUS 考虑采取适当的执法行动时，遵守这些信息要求是一个有利因素。
- **自我披露：** CFIUS 强烈鼓励从事可能构成违规行为的任何人及时提交自我披露，即使任何适用的 CFIUS 协议、法律或法规没有明确要求。自我披露应采用书面形式，并提供可能构成违规行为的完整描述，包括所有相关方。在 CFIUS 决定是否需要处罚或采取其他补救措施时，及时、完整的自我披露也将被视为有利因素。 “及时性”的一个关键因素是 CFIUS 或其他政府官员在自我披露之前是否已经或即将发

现相关行为。 CFIUS 还将考虑报告方是否遵守了任何适用的要求披露行为的 CFIUS 缓解措施。如果企业正在完成对潜在违规行为的内部调查，它仍应向 CFIUS 进行初步自我披露，然后进行完整的自我披露。

- **内幕消息：** CFIUS 鼓励各方向 CFIUS 监控和执法页面上的 CFIUS 提供热线提交内幕消息、参考讯息或其他相关信息。

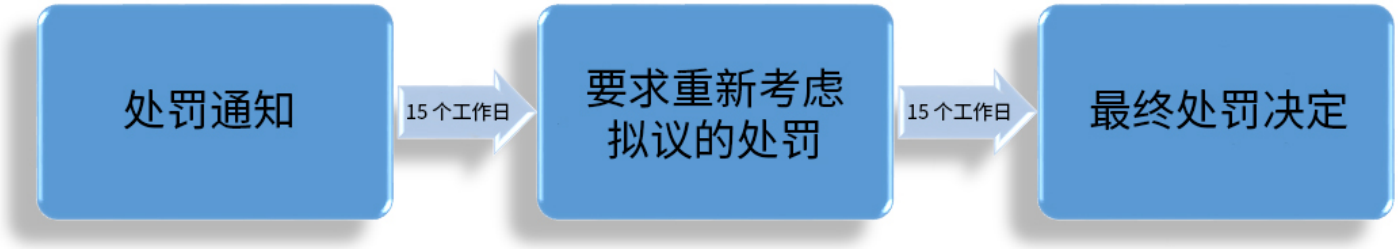
处罚流程

2018 年外国投资风险审查现代化法案 (FIRRMA) 和 CFIUS 法规规定了可根据不同违规行为评估的最高处罚。具体来说：

- 依第 31 章第 800.404 节、第 800.405 节或第 800.502 节的规定，提交有重大错误陈述或遗漏的声明或通知或提供虚假证明的任何人可能会被处以每次违规不超过 250,000 美元的民事罚款。
- 任何未能遵守第 800.401 节要求的人可能会被处以不超过 250,000 美元或交易价值的民事罚款（以两者中较高者为准）。
- 任何人故意或因重大过失违反《国防生产法》第 721(l) 条规定的缓解协议的重要规定，可能会被处以每次违规不超过 250,000 美元或交易价值的民事罚款（以两者中较高者为准）。

在每种情况下，处罚都是按违规次数计算的，这表明违规行为可以累积，这意味着 CFIUS 可能会发现不止一项违规行为，并评估高于每次违规行为的最高处罚金额。该决定应基于违规的性质。[1]

准则为处罚流程提供了在 CFR 31 章第 800.901 节中所述的路线图。首先，CFIUS 发出处罚通知，包括对将要处罚的行为和将要处以罚款的数额的书面解释。该通知将说明断定该行为构成违规行为的法律依据，并可能列出委员会考虑的任何加重和减轻因素。其次，收件人可以（但不是必须）在 15 个工作日内提交复议申请，包括任何辩护、理由、减轻处罚因素或解释（如果有正当理由，可以通过书面协议延长期限）。最后，CFIUS 将在收到申请后的 15 个工作日内（可通过书面协议延长期限）在发布最终处罚决定之前考虑收到的任何申请。



加重/减轻因素*

- 问责制和未来合规
- 对美国国家安全的危害
- 疏忽、意识和意图
- 持久性和时机
- 回应和补救
- CFIUS合规计划的复杂性
- CFIUS合规记录

*这是一个非穷尽的清单

在考虑对 CFIUS 违规行为进行处罚时，CFIUS 在其基于事实的分析中权衡了许多加重和减轻因素。下面，本提示文章重点介绍了一些最值得企业注意的事项（完整列表可在此处获得）：

- **问责制和未来的合规性：**需要对行为施加问责制并激励未来的合规性
- **危害：**违规对美国国家安全的影响
- **疏忽、意识和意图：**行为在多大程度上是由于简单疏忽、重大疏忽、故意行为或任意行为造成的；有无任何隐瞒或延迟与 CFIUS 共享相关信息的行为；以及该实体内知道或应该知道该行为的人员的资历
- **持久性和时机：**从意识到行为到 CFIUS 报告之间经过的时间长度，以及行为的频率和持续时间
- **回应和补救：**是否存在自我披露，包括向 CFIUS 报告信息的及时性、性质和范围；是否完全配合 CFIUS 的调查；以及是否对该行为进行了及时、完整和适当的补救
- **复杂程度和合规记录：**企业的历史和对 CFIUS 的熟悉程度；专门用于遵守适用法律义务的内部和外部资源（例如，法律顾问、顾问、审计员和监督员）；防止此类行为的政策、培训和程序以及此类措施失败的原因；公司内部存在的合规文化；以及了解企业的其他联邦、州、地方或外国当局在评估遵守适用法律义务的质量和充分性方面的经验

前 3 大要点

CFIUS 流程极其复杂。处罚准则与最近关于 CFIUS 审查程序中扩展因素的行政命令相结合，向公众发出了 CFIUS 加强审查并承诺保护对美国国家安全特别重要的行业部门的明确信号。现在，对 CFIUS 管辖权的分析已成为所有跨境投资或收购的*实际要求*。

与 CFIUS 的任何沟通都可能成为违规的依据。 《执法和处罚准则》明确指出，向 CFIUS 提交的任何和所有文件（无论是在评估、审查、调查、缓解或非正式磋商的背景下）都应完整、透明并及时完成。 CFIUS 在评估潜在处罚时将其中每一项都视为加重或减轻因素。

专用资源和合规承诺是缓解因素。执法和处罚准则明确指出——作为减轻处罚因素——企业专门用于遵守适用的 CFIUS 法律义务的内部和外部资源（包括法律顾问），以及为防止被禁止行为而制定的政策、培训和程序。这些因素清楚地强调了让专家对所有跨境交易进行标准 CFIUS 相关尽职调查并酌情进行 CFIUS 风险评估以全面审查所有 CFIUS 考虑因素的监管价值。

如果您对本提示文章有任何疑问或希望寻求帮助制定 CFIUS 策略，请联系作者或 Holland & Knight 的 CFIUS 和工业安全团队的其他成员。我们的律师拥有开展必要的尽职调查以确定涵盖交易的知识和经验，准备必要的 CFIUS 风险评估，为企业领导者提供评估监管风险的工具，并帮助驾驭不断变化的 CFIUS 环境。

附注：

[1] 参见 31 章 第 800.901 节。

California Expands Pay Data Reporting and Mandates Pay Scale Disclosure

By Lauren Polk, John H. Haney and Samuel J. Stone

HIGHLIGHTS:

- California Gov. Gavin Newsom signed Senate Bill (SB) 1162 on Sept. 27, 2022, to expand the requirements for annual pay data reports and requires covered employers to publish pay scales with job postings as well as to retain certain pay records.
- The law, which takes effect Jan. 1, 2023, is an effort to bolster pay transparency and counter workplace discrimination and aligns California law with several other states, including New York, Nevada and Washington.
- This Holland & Knight article covers the two distinct disclosure requirements under the new law as well as next steps employers should take to prepare for the new requirements.

California Gov. Gavin Newsom signed Senate Bill (SB) 1162 on Sept. 27, 2022, to expand the requirements for annual pay data reports and requires covered employers to publish pay scales with job postings as well as to retain certain pay records. The law, which takes effect Jan. 1, 2023, is an effort to bolster pay transparency and counter workplace discrimination and aligns California law with several other states, including New York, Nevada and Washington.

REQUIREMENTS UNDER THE LAW

There are two distinct disclosure requirements under the new law: mandatory pay scale information for job postings and expanded pay data reporting requirements.

Expanded Annual Pay Data Reporting to California Civil Rights Department

SB 1162 represents an expansion of a previous pay data reporting bill, SB 973, that went into effect in 2021. SB 973 required employers with 100 or more employees, and who were required under federal law to file an annual federal Employer Information Report (EEO-1), to submit an annual pay data report to the California Civil Rights Department (CRD, formerly known as the Department of Fair Employment and Housing (DFEH)). However, SB 973 did not address workers supplied to employers by labor contractors (e.g., staffing agencies).

Under SB 1162, covered employers who are supplied workers by labor contractors will not escape this pay data reporting obligation in 2023. The law defines labor contractors as "an individual or entity that supplies, either with or without a contract, a client employer with workers to perform labor within the employer's usual course of business." Employers who have 100 or more employees hired through labor contractors within the prior calendar year will now be required to file a separate report for those employees who have been supplied by labor contractors, and the report will need to identify the labor contractors. In turn, labor contractors will be obligated to provide pay data to the reporting employers.

SB 1162 also broadens SB 973 by requiring the median and mean hourly rate for each combination of race, ethnicity and sex in the designated job categories. Employers with multiple establishments are required to submit separate reports for each establishment instead of a consolidated report and are no longer permitted to submit an EEO-1 in lieu of the required pay data report.

Accordingly, in 2023, pay data reports must include the following:

1. The number of employees by race, ethnicity, and sex in each of the following job categories:

    a. executive or senior level officials and managers

    b. first or mid-level officials and managers

    c. professionals

    d. technicians

    e. sales workers

    f. administrative support workers

    g. craft workers

    h. operatives

    i. laborers and helpers

    j. service workers

2. Within each job category listed above, the number of employees by race, ethnicity and sex whose annual earnings fall within each of the pay bands defined by the U.S. Bureau of Labor Statistics Occupational Employment and Wage Statistics Survey based upon employees' W-2 earnings

3. Within each job category listed above, for each combination of race, ethnicity and sex, the median and mean hourly rate, based upon employees' W-2 earnings

4. The total number of hours worked by each employee counted in each pay band during the reporting year

5. For employers with multiple establishments, a report must be submitted for each establishment

An employer who fails to submit the required report to the CRD may be subject to costs associated with compelling compliance. A court may also impose civil penalties up to $100 per employee and up to $200 per employee for subsequent failures to file the pay data report.

Pay Scale Disclosure to Employees and Applicants

Beginning Jan. 1, 2023, employers with 15 or more employees must include the pay scale in all job postings under California Labor Code 432.3. "Pay scale" is defined by statute as the salary or hourly wage range that the employer reasonably expects to pay for the position. Additionally, if a covered employer posts, announces or publishes job postings using a third party, the employer must provide pay scale information to the third party

for it to include in the job posting. Further, upon request, covered employers must provide the pay scale information to current employees and to applicants upon a reasonable request.

Failure to comply with the required disclosures allows "aggrieved individuals" to file a written complaint against employers with the Labor Commissioner within one year after learning that employers did not make the required disclosures. Upon a finding that the employer violated the law, the Labor Commissioner may order the employer to pay civil penalties ranging from $100 to $10,000 per violation based on the totality of the circumstances. Notably, the Labor Commissioner will not assess a penalty upon first violation of the pay scale disclosure law upon showing that the employer updated job postings for open positions to include the required pay scale in compliance with the law. An aggrieved individual may also bring a civil action for injunctive relief and other relief as deemed appropriate by a court.

Employee Record Retention

Employers also must maintain employee records, including job titles and wage rate histories, through the term of each employee's employment and for three years after the employment has ended. As under current law, these records are subject to inspection by the Labor Commissioner.

NEXT STEPS FOR CALIFORNIA EMPLOYERS

In order to prepare for the new 2023 pay data reporting and disclosure requirements, covered employers should ensure their policies and procedures comply with the requirement to maintain pay history documentation for current employees for the required period of time and should update existing and new job postings to meet the requirements to disclose pay scale information. Employers who do not comply with the requirements to submit pay data and post pay scales within their job posting may be subject to civil penalties and costly lawsuits.

In addition, as SB 1162 extends pay data collection obligations to employees furnished by labor contractors, covered employers should also ensure they comply with the new reporting requirements for these workers. This represents a significant expansion of existing pay data requirements, and employers utilizing staffing agencies, independent contractors and/or temporary employees must consider such third-party-sourced employees in its reports. A court may apportion an appropriate amount of penalties to a labor contractor who did not provide the requisite pay data for an employer to submit a complete and accurate report.

Employers should also review agreements with staffing agencies and other third parties to ensure that employers have a contractual right to receive pay data information from their contractors for purposes of pay data reporting. Agreements with professional employer organizations (PEOs) and payroll companies should also be reviewed to ensure access to this data for the period of time required by the statute (especially after a contract with such a service provider may be terminated).

SB 1162 creates an additional layer of complex requirements and easy pitfalls for employers. All entities doing business in California should consult with counsel on current records and pay information to review and rectify potential discrepancies. For more information about how SB 1162 applies to your business, contact the authors.

加州扩大薪酬数据报告并强制披露薪酬等级

原文作者：Lauren Polk 、John H. Haney 及 Samuel J. Stone

重点摘要:

- 加州州长加文·纽森 (Gavin Newsom) 于 2022 年 9 月 27 日签署了参议院法案 (SB) 1162，以扩大对年度薪酬数据报告的要求，并要求涵盖的雇主发布带有招聘信息的薪酬等级信息，及保留某些薪酬记录。
- 该法律将于 2023 年 1 月 1 日生效，旨在提高薪酬透明度和打击工作场所歧视，并使加州法律与其他几个州（包括纽约、内华达和华盛顿州）保持一致。
- 本 Holland & Knight 提示文章涵盖了新法律规定的两项不同的披露要求，以及雇主应采取的后续步骤来为新要求做准备。

加州州长加文·纽森于 2022 年 9 月 27 日签署了参议院法案 (SB) 1162，以扩大对年度薪酬数据报告的要求，并要求涵盖的雇主发布带有招聘信息的薪酬等级信息，及保留某些薪酬记录。该法律将于 2023 年 1 月 1 日生效，旨在提高薪酬透明度和打击工作场所歧视，并使加州法律与其他几个州（包括纽约、内华达和华盛顿州）保持一致。

法律要求

新法律有两项不同的披露要求：职位发布的强制性薪酬等级信息和扩大的薪酬数据报告要求。

扩大向加州民权部门报告的年度薪酬数据

SB 1162 代表了之前的薪酬数据报告法案 SB 973 的扩展，该法案于 2021 年生效。SB 973 要求拥有 100 名或更多雇员、及根据联邦法律必须提交年度联邦雇主信息报告 (EEO) -1) 的雇主，向加州民权部（CRD，前身为公平就业和住房部（DFEH））提交年度薪酬数据报告。但是，SB 973 没有处理到由劳务承包商（例如人事代理机构）提供给雇主的员工。

根据 SB 1162，在 2023 年由劳务承包商提供员工的适用雇主将无法逃避这一薪酬数据报告义务。法律将劳务承包商定义为“无论是否签订合同，向客户雇主提供在雇主的日常业务范围内进行劳动的员工的个人或实体”。”在上一个日历年内通过劳务承包商雇用了 100 名或更多雇员的雇主现在需要为那些由劳务承包商提供的雇员提交单独的报告，并且该报告将需要显示劳务承包商。反过来，劳务承包商将有义务向报告的雇主提供薪酬数据。

SB 1162 还扩大了 SB 973，要求指定工作类别中每个种族、民族和性别组合的中位数和平均时薪。拥有多个机构的雇主必须为每个机构提交单独的报告而不是合并报告，并且不再允许提交 EEO-1 代替所需的薪酬数据报告。

因此，在 2023 年，薪酬数据报告必须包括以下内容：

1. 以下每个工作类别中按种族、民族和性别划分的雇员人数：

    a.行政或高级主管和管理人员

    b.一级或中级主管和管理人员

    c.专业人员

    d.技术人员

    e.销售人员

    f.行政支持人员

    g.工艺员工

    h.操作人員

    i.劳工和帮手

    j.服务人员

2. 在上面列出的每个工作类别中，按种族、族裔和性别划分根据员工的 W-2 收入确定属于的年收入在美国劳工统计局职业就业统计调查的每个薪酬范围内的雇员人数
3. 在上面列出的每个工作类别中，对于种族、民族和性别的每种组合，基于员工的 W-2 收入中位数和平均时薪
4. 报告年度内每个薪资范围内每位员工的总工作时数
5. 对于拥有多个机构的雇主，必须为每个机构提交一份报告

未能向 CRD 提交所需报告的雇主可能需要支付与强制合规相关的费用。法院还可以处以每一员工最高 100 美元的民事处罚，对随后未能提交薪酬数据报告处以每一员工最高 200 美元的民事处罚。

向员工和申请人披露薪酬表

从 2023 年 1 月 1 日开始，拥有 15 名或更多员工的雇主必须根据《加州劳工法》第 432.3 条在所有职位发布中加入薪级表。“薪级表”根据法规定义为雇主合理期望为该职位支付的薪水或小时工资范围。此外，如果受保护的雇主使用第三方发布、宣布或发布招聘信息，则雇主必须向第三方提供薪酬等级信息，以便将其包含在招聘信息中。此外，根据要求，涵盖的雇主必须根据合理要求向现有雇员和申请人提供薪酬等级信息。

不遵守规定的披露允许“受侵害的个人”在得知雇主未按规定披露后一年内向劳动局委员提交针对雇主的书面投诉。一旦发现雇主违反了法律，劳动局委员可命令雇主根据整体情况对每次违规行为支付 100 美元至 10,000 美元不等的民事罚款。值得注意的是，劳动局委员不会在首次违反薪酬等级披露法的情况下评估处罚，只要表明雇主更新了空缺职位的招聘信息以包括符合法律规定的薪酬等级。受侵害的个人也可以提起民事诉讼以获得禁令救济和法院认为适当的其他救济。

员工记录保留

雇主还必须在每个雇员的雇佣期限内和雇佣关系结束后的三年内保留雇员记录，包括职务和工资率历史记录。根据现行法律，这些记录须接受劳动局委员的检查。

加州雇主的下一步

为了为新的 2023 年薪酬数据报告和披露要求做好准备，涵盖的雇主应确保其政策和程序符合在规定的时间段内维护现有员工的薪酬历史记录文件的要求，并应更新现有和新的职位发布，以符合披露薪酬等级信息的要求。不遵守在招聘信息中提交薪酬数据和公布薪酬等级的要求的雇主可能会受到民事处罚和代价高昂的诉讼。

此外，由于 SB 1162 将薪酬数据收集义务扩展到劳务承包商提供的雇员，因此适用的雇主还应确保他们遵守针对这些员工的新报告要求。这代表了现有薪酬数据要求的显着扩展，使用人事代理机构、独立承包商和/或临时雇员的雇主必须在其报告中考虑此类第三方来源的雇员。法院可对未提供雇主提交完整准确报告所需的薪酬数据的劳务承包商处以适当数额的罚款。

雇主还应审查与人事代理机构和其他第三方的协议，以确保雇主有合同权利从其承包商那里接收薪酬数据信息，用于薪酬数据报告。还应审查与专业雇主组织 (PEO) 和薪资公司的协议，以确保在法规要求的期限内访问此数据（尤其是在与此类服务提供商的合同可能终止之后）。

SB 1162 为雇主增加了一层复杂的要求和容易陷入的陷阱。所有在加州开展业务的实体都应就当前记录和支付信息咨询律师，以审查和纠正潜在的差异。有关 SB 1162 如何适用于您的事业的更多信息，请联系作者。

NYDFS Proposes Amendments to Cybersecurity Regulation

By Kristen N. Ricci and Mark H. Francis

HIGHLIGHTS:

- The New York Department of Financial Services recently released Proposed Amendments to its Cybersecurity Regulation that represent a significant update to the regulation of cybersecurity practices within the financial services sector.
- The Proposed Amendments call for increased mandatory controls associated with common attack vectors and additional cybersecurity requirements for larger companies, among other enhancements.
- The comment period for the Proposed Amendments continues until Jan. 8, 2023, and most amendments become effective within 180 days of adoption.

The New York Department of Financial Services (NYDFS) on Nov. 9, 2022, released Proposed Amendments to its Cybersecurity Regulation.[1] The NYDFS Cybersecurity Regulation was one of the first laws requiring companies to comply with a prescriptive set of requirements in their cybersecurity program and has been credited for influencing similar requirements by several other regulatory bodies.

The Proposed Amendments reflect a significant update to NYDFS regulation of cybersecurity practices within the financial services sector. For example, whereas the original Cybersecurity Regulation provided organizations with more freedom in designing their cybersecurity program based on assessed risks, the Proposed Amendments now require the implementation of specific administrative and technical controls designed to address common vulnerabilities. In addition, consistent with a growing regulatory trend, the Proposed Amendments move beyond administrative and technical safeguards to regulate corporate behavior by mandating cybersecurity governance practices. Finally, the Proposed Amendments subject larger financial services companies to independent audits and external risk assessments. As discussed below, these proposed changes will likely impose significant new obligations for regulated financial services companies and increase legal compliance risks for these entities together with their executives and boards of directors.

NYDFS CYBERSECURITY REGULATIONS

NYDFS regulates financial services companies licensed to operate in New York, including banks, insurance companies and mortgage loan servicers. In 2017, the agency published its Cybersecurity Regulation, which went fully into effect in March 2019. The law required its regulated financial services companies to maintain a comprehensive cybersecurity program in accordance with a number of specific security requirements.

Specifically, companies must conduct yearly risk assessments, develop policies and procedures related to 15 information security controls based on these risk assessments, maintain incident response plans, conduct annual penetration tests and biannual vulnerability assessments, use multifactor authentication for access from an external network, notify regulators of a cybersecurity event within 72 hours, and much more. In addition to these requirements, the Chief Information Security Officer (CISO) must provide the board of directors or equivalent governing body with annual, written reports concerning the company's cybersecurity program. Regulated companies also must annually certify their compliance with the Regulations in a submission to NYDFS. The law does provide exemptions for financial services companies that have less than 20

employees/independent contractors, less than $5 million in gross annual revenue in each of its last three fiscal years or less than $15 million in year-end total assets.[2]

Since the Cybersecurity Regulation went into effect, NYDFS brought several enforcement actions for violations of these requirements. In its first public enforcement action (see Holland & Knight's previous alert, "SEC Issues First-Ever Penalties for Deficient Cybersecurity Risk Controls," June 22, 2021), NYDFS announced charges against First American Title Insurance Co. for allegedly exposing millions of consumers' sensitive personal information to the public. In that matter, NYDFS alleged that each instance of exposure of nonpublic information constitutes a separate violation carrying up to $1,000 in penalties per violation. More recently, NYDFS announced that Robinhood Crypto LLC will pay $30 million penalty to the state of New York for allegedly violating the Cybersecurity Regulation and other regulations. As illustrated by these announcements, the cost of violating the Cybersecurity Regulation can be substantial.

THE PROPOSED AMENDMENTS

On July 29, 2022, NYDFS released Draft Pre-Proposed Amendments for review and comment. The comment period for these Draft Pre-Proposed Amendments concluded on Aug. 18, 2022. After consideration of these nonpublic comments, NYDFS on Nov. 9, 2022, promulgated the Proposed Amendments through a formal New York rulemaking process, which provides a minimum 60-day public comment period. The comment period for the Proposed Amendments will run until Jan. 8, 2023. If adopted, most amendments will take effect 180 days from the date of adoption. There are different transitional periods to implement a number of technology-related amendments.

The Proposed Amendments generally fall within the following five categories: 1) increased mandatory controls associated with common attack vectors, 2) enhanced requirements for privileged accounts, 3) enhanced notification obligations, 4) expansion of cyber governance practices, and 5) additional cybersecurity requirements for larger companies. The amendments to these five categories are discussed in more details below.

1. Increased Mandatory Controls and Practices

Cybercriminals often use similar tactics, techniques and procedures to gain access into a company's network. Over the past few years, the three most common vectors used to gain access into a victim's system have been phishing emails, misconfigured remote desktop protocol (RDP)[3] and unpatched software. In addition, both the SolarWinds and Log4j vulnerabilities highlighted the need to maintain detailed inventories of the software programs and versions used throughout an organization.

In response to these common vulnerabilities, the Proposed Amendments would require regulated companies to implement mandatory controls and practices designed to address these common vulnerabilities. In an effort to address phishing emails, the Proposed Amendments require monitoring and filtering of emails to block malicious content. They also require employees to receive cybersecurity awareness training that includes social engineering exercises. To address RDP vulnerability, the Proposed Amendments require companies to develop policies and procedures related to remote access, use strong and unique passwords when employed as a method of authentication, utilize multifactor authentication for remote access, disable or securely configure all protocols that permit remote control of devices, and periodically review all user access privileges and remove accounts/accesses that are no longer necessary. Addressing the unpatched software vulnerability, the Proposed Amendments require companies to develop policies and procedures related to vulnerability and patch management, develop policies and procedures related to end-of-life management, and maintain asset inventories that would include the assets' owner, location, support expiration date, update frequency and other specifically identified information.

The Proposed Amendments also focus on protecting business operations during a ransomware attacks. Specifically, the Proposed Amendments require incident response plans to include ransomware incidents and backup recovery planning. In addition, the Proposed Amendments require companies to develop detailed business continuity and disaster recovery (BCDR) plans, which include procedures for backup of essential data and offsite storage of information. Finally, the Proposed Amendments require regulated companies to periodically test their ability to restore systems from backups.

In addition to these specific controls, policies and procedures, the Proposed Amendments require annual penetration tests by a qualified internal or external independent party and regular vulnerability assessments and automated scans of information systems to identify, analyze and report vulnerabilities.

2. Enhanced Requirement for Privileged Accounts

One of the more common tactics employed by cybercriminals upon gaining unauthorized access within a system is privilege escalation; that is, threat actors seek to gain control of user accounts that contain the highest level of access and authority within a network.

The Proposed Amendments attempt to address this concern through specific requirements related to privileged accounts. As an initial step, the Proposed Amendments define the term "privileged accounts." Essentially, a privileged account is an account within the network that has authority to make configuration changes or add/remove user accounts. The Proposed Amendments then require regulated companies to:

- limit the number of privileged accounts
- limit access to privileged accounts to only those users who need access to perform their job
- limit the use of privileged accounts to only when performing functions requiring use of such accounts
- annually review all user access privileges and remove accounts and access that are no longer necessary
- employ multifactor authentication (MFA) for all privileged accounts[4]
- promptly terminate access following departures
- implement a privileged access management solution
- implement an automated method of blocking commonly used passwords

3. Enhanced Notification Obligations

Although the Cybersecurity Regulations require regulated entities to report cybersecurity incidents within 72 hours to NYDFS, the Proposed Amendments create an additional notification obligation related to ransomware payments and would require regulated entities to notify NYDFS within 24 hours of any extortion payments made in response to a cybersecurity event. In addition, within 30 days of payment, the entity would be required to provide NYDFS a written description explaining a) why payment was necessary, b) the alternatives considered, c) the due diligence taken to assess these alternatives, and d) the due diligence taken to ensure payment complied with applicable rules and regulations, including those of the U.S. Department of the Treasury's Office of Foreign Assets Control.

In addition, within 90 days of the notice of the cybersecurity incident, regulated entities must provide the Superintendent any information requested regarding the investigation of the cybersecurity incident. The Proposed Amendments note that regulated entities have a continuing obligation to update and supplement all provided information.

4. Expansion of Cybersecurity Governance Practices

One of the key aspects of the Proposed Amendments is the expansion of cybersecurity governance practices as the NYDFS seek to hold executives and boards of directors accountable for regulated entities' cybersecurity programs.

Preliminarily, the Proposed Amendments define the term "senior governing body" to mean the regulated entities' board of directors (or an appropriate committee thereof) or an equivalent governing body.[5] The Proposed Amendment then requires regulated entities to employ the following practices:

- the senior governing body must approve the written cybersecurity policies and procedure annually
- the senior governing body must receive reports concerning the regulated entity's material cybersecurity issues
- the CISOs must timely report material cybersecurity issues to the senior governing body
- material issues found in penetration tests or vulnerability assessments must be documented and reported to the senior governing body and senior management
- the board of directors, or an appropriate committee of the board, must have sufficient expertise and knowledge, or be advised by person with sufficient expertise and knowledge, to exercise effective oversight of cyber risk and of those responsible for cybersecurity

In addition, the Proposed Amendments place increased responsibilities on the executive management and senior officers. Where regulated entities have a board of directors, the board shall exercise oversight of and provide direction to management on cybersecurity risk management and require the executive management to develop, implement and maintain the company's cybersecurity program. Regulated entities also must periodically test their incident response plan with the CEO and senior officers present and periodically test their BCDR plan with senior officers present.

Finally, the Proposed Amendments require regulated entities to submit annual certification of compliance with these Cybersecurity Regulations. If an entity is not compliant, the Proposed Amendment would require the entity to submit a written acknowledgement that it is not compliant, explain the nature and extent of its noncompliance, and provide remediation plans and timelines for implementation. Under the Proposed Amendments, the certification or written acknowledgement of noncompliance must be signed by both the CEO and CISO.

5. Additional Cybersecurity Requirements for Larger Companies

The Proposed Amendments create a new category of regulated entities called Class A companies. Class A companies are regulated entities that have at least $20 million in gross annual revenue in each of the last two fiscal years and have over 2,000 employees (including employees who work at an entity's affiliate) or make more than $1 billion in gross revenue in each of the last two fiscal years from all business operations (including gross annual revenue of an entity's affiliates). Under the Proposed Amendments, Class A companies have significantly more stringent cybersecurity requirements that require them to:

- conduct annual independent audits of their cybersecurity program
- monitor privileged access activity
- implement password vaulting for privileged accounts and an automated method of blocking commonly used passwords
- use external experts to conduct a risk assessment at least once every three years
- implement endpoint detection and response solution to monitor anomalous activity
- implement centralized logging and security event alerting

The Proposed Amendments do increase their limited exemptions provisions to exempt financial services companies that have less than 20 employees/independent contractors, less than $5 million in gross annual revenue in each of its last three fiscal years or less than $15 million in year-end total assets.

KEY TAKEAWAYS REGARDING THE PROPOSED AMENDMENTS

1. Increasing Prescriptive Requirements

Many cybersecurity and privacy regulations require entities to implement comprehensive cybersecurity programs based on assessed risks. Such requirements typically give regulated entities significant autonomy to design technical and administrative controls deemed appropriate for their environment. However, the Proposed Amendments continue to reduce such autonomy by codifying specific administrative and technical controls. Although NYDFS may have the best intentions, this approach potentially erodes regulated entities' ability to effectively allocate limited cybersecurity resources on a risk-prioritized basis, since they are forced to instead operate programs prioritized for compliance with multiple regulators' competing compliance demands. In addition, the mandatory administrative and technical controls are designed to counter today's vulnerabilities, but cyber threats constantly evolve and the codification of such practices could become outdated. It is also unclear to what extent the increased regulatory requirements will negatively impact 1) resource-limited organizations, 2) security personnel subject to ever-increasing demands and job-related risks, or 3) the ability of newer, smaller and more diverse service providers to compete for business with financial services companies imposing significant compliance and indemnity demands due to the Cybersecurity Regulations.

2. Material New Governance Oversight and Demands

There is little doubt that NYDFS desires to improve corporate governance over regulated companies' cybersecurity practices. For example, the Proposed Amendments specifically require boards of directors to approve the written cybersecurity policies and procedures, receive reports concerning material cybersecurity issues, and provide effective oversight over the entity's cybersecurity program. In addition, consistent with the approach taken by the U.S. Securities and Exchange Commission, board members will be required to have significant expertise and knowledge to exercise effective oversight of cyber risk. In doing so, however, the Proposed Amendments will materially impact the composition of boards and management teams. A potential talent shortage of cybersecurity professionals qualified to serve in such roles may be a significant issue for regulated entities. In addition, these requirements may divert funds allocated to other important environmental, social and governance (ESG) initiatives and, likewise, divert board and management seats that would otherwise be allocated to fulfill other ESG and diversity objectives.

3. Increased Legal Risk Exposure

More regulation inherently means more legal compliance risk due to regulatory enforcement and the increased likelihood of shareholder derivative suits in the event of a cybersecurity incident. For example, allegations of ineffective oversight and breach of fiduciary duties may become more common in data breach cases, and such derivative actions may identify the NYDFS regulations as setting minimum standards (i.e., the floor) required of boards with respect to their personal cybersecurity obligations.

The Proposed Amendments also increase potential legal risk for regulated entities and their senior management, such as the requirement that the CEO and CISO both sign an annual certification of compliance. In many organizations, the CEO is not an expert in cybersecurity or able to dedicate significant time to that one area, making the attestation difficult, and the dual-signatory requirement could create tension and conflicts within upper management. And certainly the certification itself could expose a regulated entity, and its CEO and CISO personally, to allegations of misrepresentation or fraud in legal actions – NYDFS has already alleged false certification against several regulated entities in enforcement actions. In addition, because the Proposed Amendments require a detailed account of any noncompliance in the written acknowledgement, good faith efforts at full disclosure could be leveraged against the entity in any subsequent legal action. This is likewise true for good faith efforts to fully document gaps identified during penetration tests or vulnerability assessments. Collectively, these new requirements pile onto the already-stressful jobs of CEOs, CISOs and board, particularly in the financial services sector, with more demands and higher personal risks.

4. Increased Compliance Costs

Once the proposed changes are adopted, significant additional resources may be needed to implement the required technical and administrative controls, governance practices, and third-party penetration testing, audits and risk assessments. There will also be practical challenges associated with the rules, such as annually testing incident response plans with all critical staff, including senior officers and the CEO. A repeating cadence of third-party audits may be expensive, time-consuming and distracting. Demands for qualified independent auditors may also result in a backlog of audit requests that challenge compliance deadlines and result in some talent loss as cybersecurity professionals move from internal programs to audit firms.

CONCLUSION

Perhaps the key question is whether the Cybersecurity Regulations have proved their value in a cost-benefit analysis since they went into effect. Do prescriptive cybersecurity requirements mitigate cybersecurity risks materially better than existing laws and entities' independently implemented cybersecurity practices, or do they result in increased compliance costs without achieving desired aims?

If you have any questions about the proposed amendments to the NYDFS Cybersecurity Regulation or need assistance submitting comments to help shape the final rule to reflect industry concerns, contact the authors or a member of Holland & Knight's Data Strategy, Security & Privacy Team.

Notes

[1] NYCRR 500.

[2] 23 NYCRR 5000.19.

[3] RDP is a communication protocol used in Microsoft operating systems to allow users to access computers remotely. As companies rapidly implemented work-from-home strategies in response to the COVID-19 pandemic, they had to allow such remote access to the companies' systems. Misconfiguration of such access resulted in a significant increase in cybercriminals gaining unauthorized access through RDP attacks.

[4] The Proposed Amendments provided do not require MFA on service accounts that prohibit interactive login as long as the CISO has approved in writing the implementation of compensating controls that achieve reasonable equivalent security.

[5] If the regulated entity does not have a board of directors or an equivalent governing body, the senior governing body refers to the senior officer responsible for the entity's cybersecurity program.

纽约州金融服务部提议修订网络安全条例

原文作者：**Kristen N. Ricci 及 Mark H. Francis**

重点摘要:

- 纽约州金融服务部最近发布了其网络安全条例的拟议修正案，这是对金融服务行业网络安全实践监管的重大更新。
- 拟议的修正案要求增加与常见攻击媒介相关的强制性控制和对大公司的额外网络安全要求，以及其他增强措施。
- 拟议修正案的评论期持续到 2023 年 1 月 8 日，大多数修正案在通过后 180 天内生效。

纽约州金融服务部 (NYDFS) 于 2022 年 11 月 9 日发布了其网络安全条例的拟议修正案。[1] NYDFS 网络安全条例是首批要求公司在其网络安全计划中遵守一套规定要求的法律之一，并因影响其他几个监管机构的类似要求而受到赞誉。

拟议修正案反映了 NYDFS 对金融服务行业网络安全实践监管的重大更新。例如，虽然最初的网络安全条例为组织提供了更多的自由来根据评估的风险设计其网络安全计划，但拟议的修正案现在要求实施旨在解决常见漏洞的特定管理和技术控制。此外，与日益增长的监管趋势一致，拟议修正案超越了行政和技术保障措施，通过强制执行网络安全治理实践来规范企业行为。最后，拟议修正案要求大型金融服务公司接受独立审计和外部风险评估。如下所述，这些拟议的变更可能会给受监管的金融服务公司带来重大的新义务，并增加这些实体及其高管和董事会的法律合规风险。

NYDFS 网络安全条例

NYDFS 监管获准在纽约州经营的金融服务公司，包括银行、保险公司和抵押贷款服务商。 2017 年，该机构发布了《网络安全条例》，该条例于 2019 年 3 月全面生效。该法律要求受监管的金融服务公司根据一些具体的安全要求维护全面的网络安全计划。

具体来说，公司必须进行年度风险评估，根据这些风险评估制定与 15 项信息安全控制相关的政策和程序、维护事件响应计划、进行年度渗透测试和一年两次的漏洞评估、使用多因素身份验证从外部网络访问、在 72 小时内向监管机构通知网络安全事件等等。除了这些要求外，首席信息安全官 (CISO) 还必须向董事会或同等管理机构提供有关公司网络安全计划的年度书面报告。受监管的公司还必须每年在向 NYDFS 提交的文件中证明其遵守法规。法律为雇员/独立承包商少于 20 人、过去三个财政年度每年总收入少于 500 万美元或年终总资产少于 1500 万美元的金融服务公司提供豁免。[2]

自网络安全条例生效以来，NYDFS 对违反这些要求的行为采取了多项执法行动。在 2021 年 6 月 22 日的首次公共执法行动中（参见 Holland & Knight 之前的提示文章，“美国证券交易委员会首次对网络安全风险控制缺陷进行处罚”），NYDFS 宣布对 First American Title Insurance Co. 提出指控，指控其暴露数百万消费者' 向公众公开敏感的个人信息。就此而言，NYDFS 声称，非公开信息的每次曝光都构成单独的违规行为，每次违规最高可处以 1,000 美元的罚款。最近，NYDFS 宣布 Robinhood Crypto LLC 将因涉嫌违反网络安全法规和其他法规而向纽约州支付 3000 万美元的罚款。正如这些公告所示，违反网络安全条例的代价可能是巨大的。

拟议的修正案

2022 年 7 月 29 日，NYDFS 发布了预提议修正案草案以供审查和评论。这些预先提议的修正案草案的评论期于 2022 年 8 月 18 日结束。在考虑了这些非公开评论后，NYDFS 于 2022 年 11 月 9 日通过正式的纽约规则制定程序颁布了提议的修正案，该程序提供了至少 60 天的公众意见征询期。拟议修正案的评论期将持续到 2023 年 1 月 8 日。如果获得通过，大多数修正案将在通过之日起 180 天后生效。有不同的过渡期来实施一些与技术相关的修正案。

拟议修正案通常分为以下五类：1) 增加与常见攻击媒介相关的强制控制、2) 对特权帐户的增强要求、3) 增强通知义务、4) 网络治理实践的扩展、以及 5) 额外的网络安全要求对于较大的公司。下文将更详细地讨论对这五个类别的修订。

1. 增加强制性控制和做法

网络犯罪分子通常使用类似的策略、技术和程序来访问公司网络。在过去的几年中，用于访问受害者系统的三种最常见的媒介是网络钓鱼电子邮件、错误配置的远程桌面协议 (RDP) [3] 和未打补丁的软件。此外，SolarWinds 和 Log4j 漏洞都强调需要维护整个组织中使用的软件程序和版本的详细清单。

为了应对这些常见漏洞，拟议修正案将要求受监管公司实施旨在解决这些常见漏洞的强制性控制和做法。为了解决网络钓鱼电子邮件，拟议修正案要求监控和过滤电子邮件以阻止恶意内容。他们还要求员工接受包括社会工程练习在内的网络安全意识培训。为解决 RDP 漏洞，拟议修正案要求公司制定与远程访问相关的政策和程序，在用作身份验证方法时使用强而独特的密码，对远程访问使用多因素身份验证，禁用或安全配置所有允许远程控制的协议设备，并定期审查所有用户访问权限并删除不再需要的帐户/访问权限。针对未打补丁的软件漏洞，拟议修正案要求公司制定与漏洞和补丁管理相关的政策和程序，制定与报废管理相关的政策和程序，并维护资产清单，其中包括资产所有者、位置、支持到期日期、更新频率和其他特定标识信息。

拟议修正案还侧重于在勒索软件攻击期间保护业务运营。具体而言，拟议修正案要求事件响应计划包括勒索软件事件和备份恢复计划。此外，拟议修正案要求公司制定详细的业务连续性和灾难恢复 (BCDR) 计划，其中包括基本数据备份和信息异地存储的程序。最后，拟议的修正案要求受监管的公司定期测试他们从备份中恢复系统的能力。

除了这些特定的控制、政策和程序之外，拟议修正案还要求由合格的内部或外部独立方进行年度渗透测试，并定期进行漏洞评估和信息系统自动扫描，以识别、分析和报告漏洞。

2. 特权帐户的增强要求

网络犯罪分子在系统内获得未经授权的访问时采用的一种更常见的策略是特权升级；也就是说，威胁行为者试图获得对网络中包含最高级别访问权限和权限的用户帐户的控制。

拟议修正案试图通过与特权帐户相关的特定要求来解决这一问题。作为第一步，拟议修正案定义了术语“特权账户”。本质上，特权帐户是网络中有权进行配置更改或添加/删除用户帐户的帐户。拟议修正案随后要求受监管公司：

- 限制特权帐户的数量
- 将对特权帐户的访问权限限制为仅需要访问权限才能执行其工作的用户
- 将特权帐户的使用限制为仅在执行需要使用此类帐户的功能时
- 每年审查所有用户访问权限并删除不再需要的帐户和访问权限
- 对所有特权帐户采用多因素身份验证 (MFA) [4]
- 离开后立即终止访问
- 实施特权访问管理解决方案
- 实施一种自动阻止常用密码的方法

3. 强化通知义务

尽管《网络安全条例》要求受监管实体在 72 小时内向 NYDFS 报告网络安全事件，但拟议修正案规定了与勒索软件支付相关的额外通知义务，并要求受监管实体在收到任何针对网络安全的勒索付款后 24 小时内通知 NYDFS 事件。此外，在付款后 30 天内，该实体将被要求向 NYDFS 提供一份书面说明，解释 a) 为什么需要付款、b) 考虑的替代方案、c) 为评估这些替代方案而采取的尽职调查、以及 d) 应有的尽职调查以确保付款符合适用的规则和条例，包括美国财政部外国资产控制办公室的规则和条例。

此外，在网络安全事件通知后 90 天内，受监管实体必须向总监提供任何要求的有关网络安全事件调查的信息。拟议修正案指出，受监管实体有持续更新和补充所有提供信息的义务。

4. 网络安全治理实践的扩展

拟议修正案的关键方面之一是扩大网络安全治理实践，因为 NYDFS 寻求让高管和董事会对受监管实体的网络安全计划负责。

初步，拟议修正案将“高级管理机构”一词定义为受监管实体的董事会（或其适当的委员会）或同等管理机构。 [5] 然后，拟议修正案要求受监管实体采用以下做法：

- 高级管理机构必须每年批准书面网络安全政策和程序
- 高级管理机构必须收到有关受监管实体的重大网络安全问题的报告

- 首席信息安全官必须及时向高级管理机构报告重大网络安全问题
- 渗透测试或漏洞评估中发现的重大问题必须记录在案并报告给高级管理机构和高级管理层
- 董事会或董事会的适当委员会必须拥有足够的专业知识和知识，或者由具有足够专业知识和知识的人提供建议，以对网络风险和负责网络安全的人员进行有效监督

此外，拟议修正案增加了执行管理层和高级管理人员的责任。如果受监管实体设有董事会，董事会应对网络安全风险管理进行监督并向管理层提供指导，并要求执行管理层制定、实施和维护公司的网络安全计划。受监管实体还必须在 首席执行官和高级管理人员在场的情况下定期测试其事件响应计划，并在高级管理人员在场的情况下定期测试其业务连续性和灾难恢复 （BCDR） 计划。

最后，拟议修正案要求受监管实体提交符合这些网络安全法规的年度证明。如果实体不合规，拟议修正案将要求该实体提交其不合规的书面确认，解释其不合规的性质和程度，并提供补救计划和实施时间表。根据拟议修正案，不合规证明或书面确认必须由首席执行官和首席信息安全官共同签署。

5. 大公司的额外网络安全要求

拟议修正案创建了一个新的受监管实体类别，称为 A 类公司。 A 类公司是受监管的实体，在过去两个财政年度每年的总收入至少为 2000 万美元，并且拥有超过 2,000 名员工（包括在实体附属公司工作的员工）或每个年度的总收入超过 10 亿美元所有业务运营的最近两个财政年度（包括实体附属公司的年度总收入）。根据拟议修正案，A 类公司的网络安全要求要严格得多，要求他们：

- 对其网络安全计划进行年度独立审计
- 监视特权访问活动
- 为特权帐户实施密码存储和阻止常用密码的自动方法
- 使用外部专家至少每三年进行一次风险评估
- 实施端点检测和响应解决方案以监控异常活动
- 实施集中式日志记录和安全事件警报

拟议修正案确实增加了其有限豁免条款，以豁免雇员/独立承包商少于 20 人、过去三个财政年度每年总收入少于 500 万美元或年终总收入少于 1500 万美元的金融服务公司资产。

关于拟议修正案的要点

1. 增加规范性要求

许多网络安全和隐私法规要求实体根据评估的风险实施全面的网络安全计划。此类要求通常赋予受监管实体很大的自主权，以设计适合其环境的技术和管理控制措施。然而，拟议修正案通过编纂具体的行政和技术控制措施继

续减少这种自主权。尽管 NYDFS 可能有最好的意图，但这种方法可能会削弱受监管实体在风险优先的基础上有效分配有限网络安全资源的能力，因为他们被迫改为运行优先满足多个监管机构竞争合规要求的计划。此外，强制性的管理和技术控制旨在应对当今的漏洞，但网络威胁不断演变，对此类做法的编纂可能已经过时。还不清楚增加的监管要求将在多大程度上对 1) 资源有限的组织产生负面影响、2) 安全人员面临不断增长的需求和与工作相关的风险、或 3) 更新、更小和更多样化服务的能力供应商与金融服务公司竞争业务，这些公司根据网络安全条例提出了严格的合规和赔偿要求。

2.重大新治理监督与诉求

毫无疑问，NYDFS 希望改进对受监管公司网络安全实践的公司治理。例如，拟议修正案特别要求董事会批准书面网络安全政策和程序，接收有关重大网络安全问题的报告，并对实体的网络安全计划进行有效监督。此外，与美国证券交易委员会采取的方法一致，董事会成员需要具备重要的专业知识和知识才能对网络风险进行有效监督。然而，在这样做的过程中，拟议修正案将对董事会和管理团队的组成产生重大影响。有资格担任此类角色的网络安全专业人员的潜在人才短缺可能是受监管实体面临的一个重大问题。此外，这些要求可能会转移分配给其他重要环境、社会和治理 (ESG) 计划的资金，同样地，转移本应分配给实现其他 ESG 和多元化目标的董事会和管理层席位。

3.法律风险暴露增加

更多的监管本质上意味着更多的法律合规风险，这是由于监管执法以及在发生网络安全事件时股东衍生诉讼的可能性增加。例如，在数据泄露案件中，监督不力和违反受托责任的指控可能会变得更加普遍，此类衍生行动可能会将 NYDFS 法规视为设定董事会在其个人网络安全义务方面所需的最低标准（即底线）。

拟议修正案还增加了受监管实体及其高级管理层的潜在法律风险，例如要求首席执行官和首席信息安全官都签署年度合规证明。在许多组织中，首席执行官不是网络安全方面的专家，也无法在该领域投入大量时间，这使得认证变得困难，而且双重签字要求可能会在高层管理人员内部造成紧张和冲突。当然，认证本身可能会使受监管实体及其首席执行官和首席信息安全官个人面临法律诉讼中的虚假陈述或欺诈指控——NYDFS 已经在执法行动中指控了几个受监管实体的虚假认证。此外，由于拟议修正案要求在书面确认中详细说明任何不合规情况，因此在任何后续法律行动中，可以利用充分披露的善意努力对付该实体。这同样适用于充分记录渗透测试或漏洞评估期间发现的差距的善意努力。总的来说，这些新要求增加了首席执行官、首席信息安全官和董事会本已压力很大的工作，尤其是在金融服务领域，要求更多，个人风险也更高。

4.合规成本增加

一旦拟议的变更被采纳，可能需要大量额外资源来实施所需的技术和管理控制、治理实践以及第三方渗透测试、审计和风险评估。规则也会带来实际挑战，例如每年与所有关键员工（包括高级管理人员和首席执行官）一起测试事件响应计划。第三方审计的重复节奏可能是昂贵、耗时和分散注意力的。对合格的独立审计师的需求也可能导致审计请求积压，挑战合规期限，并导致一些人才流失，因为网络安全专业人员从内部项目转移到审计公司。

结论

也许关键问题在于，《网络安全条例》自生效以来是否在成本效益分析中证明了其价值。规范性网络安全要求是否比现有法律和实体独立实施的网络安全实践在实质上更好地减轻了网络安全风险，或者它们是否导致合规成本增加而没有实现预期目标？

如果您对 NYDFS 网络安全条例的拟议修正案有任何疑问，或需要帮助提交评论以帮助制定最终规则以反映行业担忧，请联系作者或 Holland & Knight 数据战略、安全和隐私团队的成员。

附注：

[1] NYCRR 500。

[2] 23 NYCRR 5000.19。

[3] RDP 是 Microsoft 操作系统中使用的一种通信协议，允许用户远程访问计算机。随着公司迅速实施在家工作策略以应对 COVID-19 大流行，他们不得不允许对公司系统进行远程访问。此类访问的错误配置导致网络犯罪分子通过 RDP 攻击获得未经授权的访问的数量显着增加。

[4] 只要首席信息安全官书面批准实施可实现合理等效安全性的补偿控制，所提供的拟议修正案就不需要对禁止交互式登录的服务帐户进行多因素身份验证。

[5] 如果受监管实体没有董事会或同等管理机构，则高级管理机构是指负责该实体网络安全计划的高级官员。

About This Newsletter
有关本期刊

Information contained in this newsletter is for the general education and knowledge of our readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and resolving a legal problem. Moreover, the laws of each jurisdiction are different and are constantly changing. If you have specific questions regarding a particular fact situation, we urge you to consult competent legal counsel. Holland & Knight lawyers are available to make presentations on a wide variety of China-related issues.

本期刊所刊载的信息仅供我们的读者为一般教育及学习目的使用。本期刊并不是为作为解决某一法律问题的唯一信息来源的目的所设计，也不应被如此使用。此外，每一法律管辖区域的法律各有不同且随时在改变。如您有关于某一特别事实情况的具体法律问题，我们建议您向合适的律师咨询。美国霍兰德奈特律师事务所的律师能够对许多与中国相关的问题提出他们的看法及建议。

About the Authors
关于本期作者

Sergio A. Fontanez focuses his practice on international regulatory and compliance matters. A former presidential management fellow with the U.S. Department of State, he brings in-depth knowledge of foreign affairs and national security to address complex legal, regulatory and policy issues.

Mark H. Francis is a leading cybersecurity, data privacy and intellectual property attorney who leverages extensive technical skill and experience to provide clients with pragmatic legal guidance across a wide array of counseling, transactional and litigation matters. He has received significant recognition for his practice, and was appointed to the U.S. Department of Homeland Security (DHS) Data Privacy and Integrity Advisory Committee (DPIAC), which provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative and technological issues within the DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters.

Robert A. Friedman is a former official with the U.S. Department of State and helps clients address a range of complex legal, regulatory and policy issues that involve international trade and investment, government regulation of cross-border transactions and compliance with U.S. laws based on foreign policy and national security. He advises businesses, entrepreneurs, investors and trade associations on matters related to economic sanctions, export controls, foreign direct investment, supply chain security, customs laws, data privacy and cybersecurity, market access, anti-corruption and national security regulations.

John H. Haney represents employers in a variety of matters involving wage and hour compliance, wrongful termination, discrimination, retaliation, harassment, leave and reasonable accommodation laws, workers' compensation, employee/independent contractor classification, exempt/nonexempt employee classification, trade secret protection, reductions in force, union matters, internal investigations, executive compensation, benefits, payroll and staffing agency vendors. In addition, he has experience with employment on-boarding, corporate transactions, state and federal agency investigations, single-plaintiff actions, wage and hour class actions, Private Attorneys General Act (PAGA) representative actions, occupational safety and health regulations, and COVID-19 workplace issues.

Sulan He focuses her practice on a broad range of international trade regulatory and transactional matters. She advises clients on a variety of sanctions and compliance matters, as well as advocates for the interests of the U.S. and foreign industries before the agencies of the U.S. government. She also has experience advising companies on the Foreign Corrupt Practices Act (FCPA) and other anti-corruption laws.

Andrew K. McAllister focuses on export controls, sanctions, customs, antidumping (AD) and countervailing duties (CVD), anti-corruption and industrial security. He advises clients on U.S. export controls laws, such as the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). He has extensive experience with U.S. trade embargoes and economic sanctions administered by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the U.S. Department of State, particularly with respect to Cuba, Iran, Russia, Ukraine and Syria.

Lauren Polk focuses her practice on wage and hour, discrimination, harassment, retaliation, employee/independent contractor classification and wrongful termination issues.

Kristen N. Ricci is a data privacy and cybersecurity attorney. She leverages her experience to provide legal guidance on a wide array of counseling, transactional and incident response matters. She provides pragmatic, tailored and actionable advice across the following areas: counseling, incident response, transactions, and mergers and acquisitions.

Samuel J. Stone works with clients in a broad range of industries on sensitive, high-stakes employment and litigation matters, complex civil and government investigations, and advice-and-counsel issues. He has represented employers and individuals at all stages of litigation and appeal, including navigating and securing favorable pre-complaint resolutions, first-chairing numerous bench trials, administrative hearings and appeals, and successfully defending favorable results on appeal. He is frequently called upon to handle high-stakes trade secret and restrictive covenant litigation; whistleblower, harassment, discrimination, and retaliation claims and investigations; and wage-and-hour class and representative actions.

Antonia I. Tzinova practices in the areas of international trade, foreign direct investment and industrial security. She advises on defense and high-technology exports; U.S. trade embargoes and economic sanctions; and customs matters. She regularly represents clients before the Committee on Foreign Investment in the United States (CFIUS) and advises on measures to mitigate Foreign Ownership, Control, or Influence (FOCI) in cross border mergers and acquisitions of U.S. government and defense contractors. She counsels foreign investors on structuring investments in the defense, high-tech and critical infrastructure sectors of the U.S. economy.

Holland & Knight
美国霍兰德奈特律师事务所

Contact Our China Practice Attorneys | 与我们的 China Practice 律师联系

Primary Contacts 主要联系人：

Hongjun Zhang, Ph.D. 张红军博士
Washington, D.C.
+1.202.457.5906
hongjun.zhang@hklaw.com

Mike Chiang 蒋尚仁律师
New York | +1.212.513.3415
San Francisco | +1.415.743.6968
mike.chiang@hklaw.com

Juan M. Alcala | Austin
+1.512.954.6515
juan.alcala@hklaw.com

Leonard A. Bernstein | Philadelphia
+1.215.252.9521
leonard.bernstein@hklaw.com

Christopher W. Boyett | Miami
+1.305.789.7790
christopher.boyett.@hklaw.com

Vito A. Costanzo | Los Angeles
+1.213.896.2409
vito.costanzo@hklaw.com

Josias N. Dewey | Miami
+1.305.789.7746
joe.dewey@hklaw.com

R. David Donoghue | Chicago
+1.312.578.6553
david.donoghue@hklaw.com

Jonathan M. Epstein | Washington, D.C.
+1.202.828.1870
jonathan.epstein@hklaw.com

Leonard H. Gilbert | Tampa
+1.813.227.6481
leonard.gilbert@hklaw.com

Enrique Gomez-Pinzon | Bogotá
+57.601.745.5800
enrique.gomezpinzon@hklaw.com

Paul J. Jaskot | Philadelphia
+1.215.252.9539
paul.jaskot@hklaw.com

Adolfo Jimenez | Miami
+1.305.789.7720
adolfo.jimenez@hklaw.com

Roth Kehoe | Atlanta
+1.404.817.8519
roth.kehoe@hklaw.com

Robert J. Labate | San Francisco
+1.415.743.6991
robert.labate@hklaw.com

Alejandro Landa Thierry | Mexico City
+52.55.3602.8002
alejandro.landa@hklaw.com

Jeffrey W. Mittleman | Boston
+1.617.854.1411
jeffrey.mittleman@hklaw.com

Anita M. Mosner | Washington, D.C.
+1.202.419.2604
anita.mosner@hklaw.com

Ronald A. Oleynik | Washington, D.C.
+1.202.457.7183
ron.oleynik@hklaw.com

Douglas A. Praw | Los Angeles
+1.213.896.2588
doug.praw@hklaw.com

John F. Pritchard | New York
+1.212.513.3233
john.pritchard@hklaw.com

Robert Ricketts | London
+44.20.7071.9910
robert.ricketts@hklaw.com

Luis Rubio Barnetche | Mexico City
+52.55.3602.8006
luis.rubio@hklaw.com

Francisco J. Sanchez | Tampa
+1.813.227.6559
francisco.sanchez@hklaw.com

Evan S. Seideman | Stamford
+1.203.905.4518
evan.seideman@hklaw.com

Jeffrey R. Seul | Boston
+1.617.305.2121
jeff.seul@hklaw.com

Vivian Thoreen | Los Angeles
+1.213.896.2482
vivian.thoreen@hklaw.com

Shawn M. Turner | Denver
+1.303.974.6645
shawn.turner@hklaw.com

Matthew P. Vafidis | San Francisco
+1.415.743.6950
matthew.vafidis@hklaw.com

Stacey H. Wang | Los Angeles
+1.213.896.2480
stacey.wang@hklaw.com

Charles A. Weiss | New York
+1.212.513.3551
charles.weiss@hklaw.com

Jose V. Zapata | Bogotá
+57.601.745.5940
jose.zapata@hklaw.co

Office Locations 办公室地点

Algiers | Atlanta | Austin | Bogotá | Boston | Century City | Charlotte | Chicago | Dallas | Denver | Fort Lauderdale
Fort Worth | Houston | Jacksonville | London | Los Angeles | Mexico City | Miami | Monterrey | New York | Orange County
Orlando | Philadelphia | Portland | Richmond | San Francisco | Stamford | Tallahassee | Tampa | Tysons | Washington, D.C.
West Palm Beach