SQUIRE SANDERS

网络安全更新

自2014年起，美国监管领域中与网络安全、数据保护、以及隐私相关的部分已产生许多发展。此外，大量塔吉特公司数据被广泛公开的外泄，引起全球公司及个人对网络安全风险以及潜在损害的关注，预计该信息泄露的损失可达7亿美元。

欧洲的监管制度主要是从个人隐私保护的角度来关注网络安全，美国政府机构的监管趋势是关注于整个网络安全标准、关键基础设施的保护。不仅是对个人隐私信息的保护，也是对技术数据、国防和重要行业的保护。

美国国防部的最终规则：保护非保密受控制技术信息

美国国防部（DOD）在2013年11月末推出第一个监管活动，根据《联邦采办条例国防部补充条例》（DFARS）“保护非保密受控制技术信息”（DFARS案例2011-D039）发布最终规则。除DFARS之外，该最终规则要求 (i) DOD承包人中的私营企业完成足够的安全措施来保护承包人信息系统中的“非保密受控制技术信息”免受未授权访问或信息披露的危害，以及 (ii) 规定就某些存在于，或通过承包人非保密信息系统影响到“非保护受控制技术信息”的网络入侵活活动向DOD强制报告。新规则不仅适用于直接与DOD签订合同的公司，也适用于任何处理或控制“非保密受控制技术信息”的转承包商(任何级别)，包括，如该规则序文中明确提到的，转承包商例如为信息提供数据托管的云存储供应商。

涵盖何种类型的数据或信息?

该规则阐明非保密受控制技术信息为“受限于访问、使用、复制、修改、履行、展示、发布、披露或传播控制的含有军事或太空应用的技术信息。”技术信息是技术数据或电脑软件，并且包括检索和工程数据、工程图纸和相关列表、规范、标准、工艺流程单、指南、技术报告、技术指令、类别物品标识、数据集、研究和分析以及相关信息，计算机软件可执行代码和源代码。受控制技术信息需要根据DOD指导5230.24“技术文件发行说明”进行识别。该条款不包含依法公开不设限制的信息。

任何掌握技术信息的企业第一步应估测该企业处理或持有“非公开受控制技术信息”的范围，不论是为其自己业务目的，还是为其他企业提供部分服务。

根据该规则，企业控制或持有非保密受控制技术信息的法义务是什么?

(1) 充足的安全性要求-对于受限于该规则的第一个要求是**“为其非保密信息系统中的非保密受控制技术信息提供充足 的安全性使其免受未授权访问和泄露威胁”的义务。该规 则并没有定义“充足的安全性”**，但是简单的阐明“充足 的安全性”意味着“与损失、滥用或未授权访问、信息修改 的后果和可能性相适应的保护措施。”然而，该规则设定了需要满足的最低标准，包括：

- 完成其项目、公司或公司范围内的未保密信息技术系统的信息系统安全，该系统中可能会存在未保密控制技术信息，或者未保密控制技术信息通过该系统传送；
- 遵守试用的（如该规则中所列）国家标准技术局（NIST）特种出版物（SP）800-53安全控制，或者，如果没有完成这些标准，企业必须向机构证明该项失败是合理的，并且解释其他的替代控制是怎样达到同等保护的；以及
- 此类由企业合理决定的额外信息系统安全要求的应用，可能会被要求在基于可评估的风险或易攻击性的动态环境中提供充足的安全性。

除了该规则中所陈述的特别标准，企业应考虑使用近期发行的“NIST”网络安全框架作为指导来评估他们的信息系统安全，并完成“充足安全性”证明。

(2) 72小时报告要求-DFARS规则的第二个要求规定任何认为自己可能遭受一项“可报告的网络事件”的企业，**要在事件发生的72小时内尽可能多的报告他们能够获得某些详细信息。**报告必须通过http:// dibnet.dod.mil. 提交。

该规则广泛的定义一项“可报告的网络事件”为（i）一个包含泄露、篡改或其他损失可能性，或危害任何存在于或通过承包人或其转承包商的非保密信息系统传播的非保密受控制技术信息，以及（ii）任何其他包含未授权访问承包人的非保密信息系统（其中存在非保密受控制技术信息或传播非保密受控制技术信息）的事件。

该规则要求报告的特别信息包括：

- 邓氏编码（DUNS）；
- 受影响的合同号，除非公司所有合同都受到影响；
- 如果事件的地点与主要承包人地点不一致，提供设备、商业和政府机构（CAGE）代码；
- 如果其与受益管理系统（地址、职位、电话、电子邮箱）中的联络方法记录的不同，请提供联络方法；
- 合同签订官联络方法（地址、职位、电话、电子邮箱）；
- 合同许可证级别；
- 转承包商姓名，以及CAGE代码，如果这是发生在转承包商网络中的事件；
- 所涉及的DOD项目、平台或系统。
- 危害的位置
- 事件发现的日期
- 危害的类型（例如，未授权访问，疏忽泄露，其他）；
- 受危害技术信息的描述；
- 与该信息危害相关的任何附加信息。compromise.

应该注意到，通过指出企业“尽可能多的”报告他们所能获得的[详细]信息，这条规则非常强调报告事件的及时性，而不是信息的完整性，并认识到72小时的时间可能并不足以使企业充分发掘出详细的信息。

该规则规定其不会根据合同、法规或其他政府规章免除或改变任何其他报告要求。

(3) 随后的评估支持要求 – 该规则的第三个要求是规定在报告网络事件之后，企业应财务某些措施来支持政府的损害评估。这些义务包括：

- 企业对其非保密网络进行进一步审查的义务，从而来寻找由网络事件而引发的损害证据,包括但不限于，识别被入侵的电脑、服务器、特殊数据以及用户账户。这包含分析作为受入侵一部分的信息系统的能力，也包含网络中被评估为入侵结果的其他信息系统；
- 企业必须审查在网络事件中被访问的数据以此来识别特定的与DOD项目、系统或合同（包括局势项目、系统和技术）相关的非保密受控制技术信息；
- 企业必须保存并保护已知受影响信息系统的图像以及从网络事件发生之后90天的所有相关的监视/数据包分析，从而允许DOD请求信息或拒绝权益；
- 如果DOD选择进行损害评估，政府可能会要求企业提供所有上述的损害评估信息。共享文件和图像的要求受限于有限的例外情况，即当有其他法律限制某企业共享数字媒体的能力时，但是如果这样的例外被提出，企业必须告知政府该项请求的来源、属性以及此类限制的描述和权威负责人。

(4) 合同的流通要求 – 该规则的最后要求规定企业必须包含一合规要求作为所有转承包商在进行商业物品交易中的强制性流通条款。尽管规则中并没有明确陈述，在采纳该规则的监管序文中评论中似乎阐明此条流通要求基金适用于那些处理或控制非保密受控制技术信息的转承包商，这个类别中不仅包含涉及相关政府合同的转承包商，也包含其他第三方提供使其可以接触到此类信息的服务的供应商—例如各种信息技术服务供应商，他们作为整体向企业提供信息技术服务而不仅仅属于相关的政府合同。

该规则的其他重要方面

当发布最终规定时，美国联邦注册公告的序文也阐明公司可能会遇到的许多相关问题。

- 序文确认，互联网服务供应商（ISPs）以及云服务供应商被认为是转包商，并且企业必须确保这些转承包商遵守规则。
- 序文确认合同管理办公室负责评估合规，并且某合同的合同办公室可以根据此类官方裁量，要求进行审查或审计来确认合规。 当根据联邦《成本会计标准》确认合规费用为一项许可成本的机会被拒绝时，序文明确包含一个声明：该规则并没有规定此类成本是不被允许的，合规的费用因此可以根据FAR（FAR31.201-2）以及DFARs(DFAR231)管理许可成本来评估。序言中的其他注释表明政府期望在很多情况中，合规费用会被分配到多个合同中，因此对于间接的成本库就是被许可和收取的。
- 序文确认如果大学和学术机构处理非保密受控制的技术信息，那么他们并不会受到该规则的豁免。
- 该规则，正如最初所提议的，不仅包含非保密受控制技术信息作为受限于该规则的数据类型，也包含数种其他信息种类，例如个人识别信息，包括HIPPA信息。这些其他信息种类在最终版本中被移除了。
- 序言表明关于报告和其他程序的附件指导说明会在未来通过对DFARS程序、指导、信息（PGI）补充的形式在http:// www.acq.osd.mil/dpap/dars/的“发布通知”一栏发布，但是并没有表明何时会发布这些指导说明。
- 该规则对主承包人和转承包人都施加了报告要求，并且序文评论道当转承包人发生一件需报告的网络事件时，尽管转承包人也做出报告，但主承包人仍有报告义务。这意味着，主承包人应确保除了所要求的流通条款中包含的内容，主承包人应明确要求转承包人在其直接通知DOD的同时告知主承包人。

联系人

Robert B. Webb III
合伙人
北维吉尼亚州
T +1 703 720 7855
E robert.webb@squiresanders.com

陆大安
合伙人
上海
T + 86 21 6103 6309
E daniel.roules@squiresanders.com

廖钰燕
合伙人
北京
T + 86 10 6589 3750
E jenny.liu@squiresanders.com