工业信息安全监测应急支撑单位

申请书

申请单位：

（加盖公章）

申请日期： 年 月 日

二零二三年十月

填写须知

申请单位应依据《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家网络安全事件应急预案》、《工业控制系统信息安全事件应急管理工作指南》等有关法规文件的要求填报。申请单位在正式填写本申请书前，需认真阅读并理解以下内容。

* 1. 申请单位应如实填报各项内容。要求文字简洁，所提供资料必须详细、真实、完整，内容不得涉及国家秘密。
  2. 部分附件或证明材料如需复印或扫描，请确保内容清晰无缺失。
  3. **提交方式及时间如下：**将申报材料电子版发送至邮箱nisia\_yj@163.com，也可以选择寄送光盘至国家工业信息安全发展研究中心（北京市石景山区鲁谷路35号），文档命名方式为“申请单位名称—监测应急支撑单位申请书”。为方便专家审阅，申请书电子版需包含word、pdf两种格式。**截止时间为：2023年10月31日。**
  4. 材料包含三份文件：1.附件1工业信息安全监测应急支撑单位申请书（word）2.附件1工业信息安全监测应急支撑单位申请书（pdf扫描版关键页盖章）3.附件2工业信息安全监测应急支撑单位申请信息汇总表（excel）
  5. 国家工业信息安全发展研究中心承诺对申请单位所提交的涉及商业秘密的材料予以保密。

承诺书

我公司/单位自愿参加由国家工业信息安全发展研究中心组织的工业信息安全监测应急支撑单位的评估认定工作，保证向中心提交的材料和信息全部真实。如发现有虚假信息或故意隐瞒情况，中心有权取消我公司/单位的评估认定资格，或在入选后取消我公司/单位的工业信息安全监测应急支撑单位称号，我公司/单位愿意承担由此引起的一切后果。

申请单位（盖章）：

法人（签字）：

年 月 日

一、工业信息安全监测应急支撑单位申请表

| **单位基本信息** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **单位名称** |  | | | | | |
| **单位地址** |  | | | | | |
| **法定代表人** |  | | **身份证号** | |  | |
| **单位性质** |  | | **组织机构代码** | |  | |
| **成立时间** |  | | **注册资本（万元）** | |  | |
| **注册地点** |  | | **注册登记号** | |  | |
| **参加的工业信息安全技术竞赛名称** |  | | **名次** | |  | |
| **资本构成情况** |  | | | | | |
| **现有资产状况** |  | | | | | |
| **近三年业绩状况** |  | | | | | |
| **子公司或分支机构** | 填写名称、地址。若无子公司或分支结构，填“无”。 | | | | | |
| **资信记录** | 在国家企业信息信用公示系统中有无不良记录 | | | | | |
| **公司人员情况** | 总人数 XX 人，从事网络安全监测应急人员 XX 人，其中本科以上学历XX 人，比例 %，具有信息安全服务资质XX人。 | | | | | |
| **办公场地情况** | □租用 XX 位置，面积约XX 平米  □购买 XX位置， 面积约XX 平米  □购买 XX位置，面积约 XX 平米 | | | | | |
| **申请单位联系方式** | | | | | | |
| **单位工业信息安全**  **监测应急工作负责人** | **姓名** |  | | **职务** | |  |
| **手机** |  | | **办公电话** | |  |
| **身份证号** |  | | | | |
| **本次评估认定负责人** | **姓名** |  | | **职务** | |  |
| **手机** |  | | **办公电话** | |  |
| **身份证号** |  | | | | |
| **邮箱** |  | | | | |
| **本次评估认定联系人** | **姓名** |  | | **职务** | |  |
| **手机** |  | | **办公电话** | |  |
| **身份证号** |  | | | | |
| **邮箱** |  | | | | |
| **主要服务地区** |  | | | | | |
| **主要服务行业** |  | | | | | |
| **申请单位**  **盖章** | （盖 章）  年 月 日 | | | | | |

二、法律地位证明（见第XX页至XX页）

说明：用于证明本单位是在中华人民共和国境内注册的独立法人组织，发展历程清晰，产权关系明确。例如独立法人证书、营业执照、组织机构代码证复印件等（三证合一的企业只需提供营业执照复印件），扫描件附在相应条目下。

1. 独立法人证书
2. 营业执照
3. 组织机构代码证
4. ……

三、办公场所证明（见第XX页至XX页）

说明：用于证明本单位拥有长期固定的办公场所和相适应的办公条件（地址、面积、设备），能够满足机构设置及业务需要。例如办公场所产权证或租赁合同关键页等，扫描件在相应条目下。

1. 产权证（或租赁合同关键页）

四、申请单位规模和财务资信证明（见第XX页至XX页）

说明：介绍本单位目前规模与资产情况，近三年来业绩说明，并提供在中华人民共和国境内登记注册的会计师事务所出具的近三年来财务审计报告，用于证明本单位近三年来经营状况良好，财务数据真实可信。

1. 本单位规模与资产状况
2. 近三年来取得的业绩（文字描述后，可附业绩证明材料，如合同关键页等）
3. 财务审计报告（近三年，附扫描件，请确保扫描件内容清晰无缺失）

五、申请单位组织结构介绍（见第XX页至XX页）

说明：介绍本单位的组织或管理结构现状、负责工业信息安全监测应急的部门组织或管理结构情况、监管体系情况等。如在全国设有分支机构，请说明分支机构情况，并提供详细信息。

1. 申请单位组织结构（文字描述，附组织架构图）
2. 工业信息安全监测应急部门组织结构（文字描述，附组织架构图）
3. 分支机构情况

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **分支机构名称** | **办公地点** | **负责人** | **联系方式** | **总人数/服务人数** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

六、申请单位工业信息安全监测应急资质证明（见第XX页至XX页）

说明：介绍申请单位取得的与网络安全、工业信息安全服务相关的资质，并提供相关资质证书和证明材料。

1. 资质证书和证明材料列表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **证书名称** | **证书编号** | **颁发单位** | **授予单位** | **有效期** | **备注** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. 资质证书和证明材料（附扫描件）

七、人员构成与素质介绍（见第XX页至XX页）

1. 申请单位人员总体情况

说明：介绍本单位现有人员数量、学历、年龄分布等情况，尤其是从事工业信息安全监测应急的项目管理人员和技术人员数量、年龄分布、在工业信息安全领域从业时长、技术人员取得相关技术或服务资质的情况等。

本单位共有XX人，…………。其中，从事工业信息安全监测应急的人员有XX人，具体情况详见列表。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **项目** | **明细** | | | | | **备注** |
| 人员教育程度 | 总人数 | 博士 | 硕士 | 本科 | 专科及以下 |  |
|  |  |  |  |  |  |
| 比例（%） |  |  |  |  |  |
| 人员年龄分布 | 总人数 | 30岁以下 | 30-40岁 | 40-50岁 | 50岁以上 |  |
|  |  |  |  |  |  |
| 比例（%） |  |  |  |  |  |
| 人员部门分布 | 部门 | 项目管理人员 | 技术人员 | 具备监测应急资质人员 | 从事信息安全2年以上 |  |
| 人力资源部 |  |  |  |  |  |
| 网络信息  安全部 |  |  |  |  |  |
| … |  |  |  |  |  |
|  | 合计 |  |  |  |  |  |

1. 监测应急部门人员情况

说明：按列表填写从事工业信息安全监测应急人员的详细信息，并提供信息安全服务相关资质证书材料。正式人员数量不少于10人，本科及以上学历人员比例不低于60%；至少6人具备工业信息安全、网络安全等相关专业技术资质，和2年以上工业信息安全、网络安全监测应急工作经验；遵纪守法，无不良行为记录，通过人员背景审查；接受过安全保密教育，签订了安全保密协议。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **部门** | **姓名** | **身份证号** | **学历/职称** | **毕业院校** | **专业** | **在本单位工作时长** | **岗位** | **技术特长** | **资质证书名称** | **资质证书编号** | **资质证书有效期** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

1. 监测应急人员工作及资质证明

说明：按监测应急部门人员列表顺序，分别提供人员的工作证或劳动合同扫描件，资质证书扫描件。

1. 姓名-证书名称
2. 姓名-证书名称
3. 姓名-证书名称
4. ……

八、单位保密及项目管理制度介绍（见第XX页至XX页）

说明：介绍本单位的保密管理制度（包括涉密资质、单位在项目实施过程中对商业秘密的相关管理制度）及监管体系情况、对本单位人员的保密要求和教育情况、本单位人员遵守国家法律法规情况，本单位涵盖工业信息安全监测应急的质量管理体系情况和技术服务管理体系情况，并提供相关证明，例如相关证明文件、所制订的保密管理制度、与本单位人员签订的保密协议或承诺书、项目管理制度、文档管理制度、服务规范化要求或标准文档等。

九、项目案例及业绩介绍（见第XX页至XX页）

1. 业绩介绍

说明：请列举本单位近3年来所完成的网络安全、工业信息安全监测应急相关项目情况，包括项目名称、时限、金额、客户名称等，如果监测应急内容是作为某个项目的一部分，应将监测应急相关的金额单独标出。同时，请从中选择5至8个项目进行详细介绍，包括所签订的合作协议（双方基本信息、合同金额、合作内容、服务要求等关键部分），针对每个项目选择1个具体的监测应急处理案例，**详细介绍该案例的具体情况、监测预警、应急响应处理流程和各环节具体处理措施**。此外，还可以从日常工作中处理的一些重大高危安全事件中挑选1至2个例子进行详细介绍（但非必须）。

**1.监测应急相关项目总体情况**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **客户名称** | **服务类别** | **实施地区** | **所属行业** | **合同金额** | **服务金额** | **主要服务内容** | **合同签订时间** | **项目验收时间** |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |
| 合计 | |  |  |  |  |  |  |  |  |  |

注：服务类别包括：安全集成、应急处理、风险评估、安全运维等。

**2.监测应急响应项目案例**（5-8个）

（1）XXX项目

（2）XXX项目

（3）XXX项目

（4）XXX项目

（5）XXX项目

**3.重大安全事件支撑案例**（1-2个，非必须）

1. 业绩证明

附所挑选项目的合作协议关键页证明，以及开展相关工作的证明材料等。

十、监测预警、应急处理能力介绍（见第XX页至XX页）

说明：介绍本单位的工业信息安全监测应急处理能力，包括主要服务的地区、行业等，是否具备独立的测试环境以及必备的软硬件设备，是否具备承担工业信息安全服务所需的安全工具，如漏洞扫描工具、渗透测试工具、协议分析工具等，是否获得过原创漏洞证书（若有提供证明材料），是否定期开展技术交流或培训，是否关注国内外前沿信息安全技术或动态等，提供培训记录表、签到表等证明材料。

（一）监测预警、应急处理能力

（二）技术交流或培训情况介绍

十一、未来服务计划（见第XX页至XX页）

说明：如本单位入选后，计划如何与中心在工业信息安全领域开展合作，支撑中心业务工作。服务计划应结合本单位实际技术能力与服务能力展开，合作领域包括但不限于监测预警、事件处置、应急演练、人员培训、漏洞报送、威胁信息报送、检查评估、标准制定、应急预案制定等环节。