为贯彻落实习近平总书记关于建设网络强国等重要指示精神，全力做好国庆70周年等国家重大活动网络安全保障工作，2019年6月，我部将作为防守方，配合国家网络安全主管部门开展网络攻防实战演习。为切实做好演习工作，现将有关内容通知如下：

1. 演习目的

通过演习，及时发现并整改我部关键信息基础设施、重要信息系统和网络存在的安全问题和隐患，加强网络安全防护能力，完善网络安全事件应急处置、通报机制，提升协同应急处置能力，确保新中国成立70周年大庆期间网络安全。

1. 演习总体安排
2. 演习准备阶段

5月10日-24日，各单位按照《演习任务工作清单》（附件1）自查、整改本单位存在的网络安全风险隐患，制定专项应急预案，提高安全意识，做好迎战准备工作。

1. 预演阶段

5月25日-31日，网信办组织开展部系统内网络攻防预演习，各单位积极参与，完成预演习中的监控、通报、整改等工作任务。

1. 实战演习阶段

6月1日-30日，作为防守方参与实战演习，各单位组织监测预警和应急处置，及时向网信办报送情况，迅速消除安全隐患，配合网信办开展追踪溯源工作。

三、演习工作要求

1. **高度重视加强领导。**各单位要高度重视本次演习工作，站在维护国家网络空间安全的高度，对演习工作进行专项部署，落实责任部门和责任人。部网信办组织信息中心相关人员、各单位网络安全联络员共同组成联合工作组，部网信办负责统筹协调、监督检查工作任务落实情况，信息中心负责提供总体技术支持保障，各安全联络员负责落实本单位工作任务，协调单位内部工作开展。
2. **严格落实各项任务。**各单位须贯彻执行本次演习的各项工作任务，严格按照时间安排向部网信办反馈信息，密切配合信息中心完成各项安全防护措施的实施，并于5月27日前填报《演习工作任务落实情况表》（附件2）正式报送部网信办（电子版发送至报送邮箱）。
3. **强化应急协调联动。**各单位应加强协调配合，提高问题处理与应急处置效率，遇到突发情况及时向部网信办报告。在演习期间，启动网络安全事件“零报告”制度，每日 16 时前网络安全联络员通过“生态环境安全运维”微信公众号报送当日本单位网络安全情况，做到有事报情况，无事报平安。
4. 其他重要事项
5. **停止网络安全调整。**为保障网络及信息系统的安全稳定运行，6月1日起停止网络安全调整、系统上线发布等工作，停止生态环境云中虚拟服务器添加、删除的自助服务，避免变更操作导致出现新的安全问题。
6. **清理互联网发布服务。**5月24日起，停止未完成系统情况填报、ICP备案等不符合互联网发布条件的系统的互联网发布服务。
7. **网络访问策略调整。**5月24日依据各单位填报的系统情况，对专网、互联网边界安全策略进行调整，如有漏报、误报的系统，将影响专网、互联网访问。
8. **虚拟服务器登录操作。**5月24日起，生态环境云虚拟服务器统一采用堡垒主机的方式进行登录操作，并停止支持其它一切登录方式。
9. **安全事件应急处置。**演习期间，在发生安全事件应急处置时，事故系统一律实行第一时间先下线、再整改，经复测完成后，恢复上线运行。
10. 联系人

网 信 办：陈 鹏 （010）66103147

信息中心：秦 宇 （010）66556088

技术支持：周海洋 18513852715

报送邮箱：security@mee.gov.cn

附件：1. 演习工作任务清单

2. 演习工作任务落实情况表

 生态环境部办公厅

2019年5月10日

附件1

演习工作任务清单

| **序号** | **任务名称** | **完成时间** | **任务内容** |
| --- | --- | --- | --- |
| **（一）系统核查清理** |
| 1 | 系统清查下线 | 5月20日 | 全面梳理本单位所管理的信息系统，关闭不再使用的系统及网站，对6月内无业务运行或不重要的系统及网站可暂做下线处理，对无用的邮箱账户进行清理。 |
| 2 | 互联网发布系统清理 | 5月24日 | 逐一排查本单位所有互联网发布系统，停止不必要的系统发布，针对将系统管理后台、数据库等发布到互联网的情况进行整改，生态环境云中系统须全部统一由信息中心互联网出口发布。 |
| 3 | 互联网发布系统备案 | 5月24日 | 按照工信部信息通信管理局的ICP备案要求，自行开展互联网发布系统的ICP备案工作（备案指南见附1） |
| **（二）安全边界防护** |
| 1 | 加强网络边界防护 | 5月20日 | 结合本单位实际情况，梳理并细化互联网、专网等边界防护墙策略配置，做好与部专网节点的安全隔离。 |
| 2 | 信息系统核查 | 5月15日 | 逐一核对本单位在生态环境云中的所有信息系统，梳理访问端口及互联网发布等信息，并根据实际情况填写《生态环境云信息系统情况表》（附2），配合信息中心做好防火墙策略细化实施 |
| **（三）系统安全加固** |
| 1 | 弱口令专项整改 | 5月24日 | 全面排查信息系统安全隐患，针对系统弱口令问题进行重点清查与整改，对所有设备、操作系统、数据库、中间件、信息系统及工作邮件系统管理后台的登陆密码进行全面更换。对信息系统及管理后台登陆的密码复杂度进行强制设置整改（密码长度不得低于8位，由字母、数字、符号组成），从根本上消除弱口令隐患。 |
| 2 | 堡垒主机配置实施 | 5月24日 | 与信息中心联系完成堡垒主机账户创建，配合信息中心完成堡垒主机的配置实施，通过堡垒主机实现生态环境云虚拟服务器的登录。 |
| 3 | 系统漏洞整改修复 | 持续开展 | 在收到信息中心下发的系统及应用安全漏洞检测报告后三个工作日内完成所有修复、整改工作。 |
| **（四）监控应急值守** |
| 1 | 实时安全监控 | 持续开展 | 演习期间，密切做好本单位网络、信息系统运行状况的实时监控，并对监测发现的问题及隐患第一时间整改，并将有关情况及时上报部网信办。 |
| 2 | 应急值守保障 | 持续开展 | 制定本单位应急处置预案与应急值守计划，做好随时处置安全事件的准备，一旦发生安全事件确保第一时间响应，第一时间处置恢复，应急值守计划报网信办。 |
| （**五）提高安全意识** |
| 1 | 提高安全意识 | 5月24日 | 对本单位网络及系统运维人员、全体职工开展网络安全宣贯教育，落实安全责任，重点强调钓鱼邮件、不明移动存储使用、弱口令等典型安全隐患，提高全员安全意识。 |

附1

ICP备案指南

**一、备案流程**

1.前往中国联通北京分公司（北京市西城区复兴门南大街6号）一层备案室，领取备案表格(核验单、登记单、信息安全责任书等，表上均有联通水印)。

2.填写上述表格，准备相关材料（详见“网站备案准备材料”）。

3.前往中国联通北京分公司备案室提交相关材料，由联通初审并代为完成备案的网上登记，将备案信息提交到北京市通信管理局审核，审核时间需10-20个工作日。

4.收到联通审核通过的通知后，将ICP备案号在嵌入到系统发布页面中。

**二、备案相关信息**

**1、联系电话**

中国联通北京分公司备案科：010-66156128（吴老师）

北京市通信管理局备案科：010-63310094

**2、网站备案准备文件**

（1）营业执照、事业法人证书、统一社会信用代码证书、社团法人证书副本复印件（如单位名称已变更，需提交行业主管部门变更证明）

（2）法人身份证复印件（或护照）

（3）网站负责人身份证原件及复印件（或护照）

（4）加盖本单位公章的网站负责人的任职证明

（5）加盖本单位公章的域名证书复印件（域名注册人需与备案单位名称一致，不一致不予受理）

（6）现场填写加盖本单位公章的核验单、登记单、信息安全责任书。

（7）网站负责人现场照片

（8）需要提供的信息：（填单子用）

法人、网站负责人的座机、手机、邮箱

北京联通IP地址

接入方式：如专线、主机托管、虚拟主机等

如需办理网站接入，需自行提供网络备案密码（当时发给法人的六位数密码）

（9）所有复印件均需为彩色，要求1:1大小，用A4纸，第（1）、（2）、（3）项请勿盖章，请勿写任何字迹

（10）用户提供的证件和加盖的公章必须清晰有效。

另外，还应带上单位成立的批复文件和网站域名信息表

，用于证明前去备案的单位是生态环境部下属单位，可以使用生态环境部信息中心的互联网IP发布。

附2

生态环境云信息系统情况表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **系统名称** | **虚拟化服务器专网地址** | **互联网发布地址** | **访问域名** | **发布端口** | **端口用途** | **互联网访问URL** |
| 1 | 华南督察局办公自动化平台 | 10.100.228.244 | 无 | http://10.100.248.244:8000/oa/ | 8000 | 系统发布 | 无 |
| 55001 | 管理端口 | 无 |
|  |  | http://10.100.248.244/UserPortalCenter/Home/Index | 80 | 系统发布 | 无 |
| 10.100.248.245 | 无 | 无 | 1433 | 数据交换 | 无 |
| 55001 | 管理端口 | 无 |
| 2 | 国控重点污染源在线监控系统 | 10.100.248.42 | 无 | http://10.100.248.42:8080/ | 8080 | 系统发布 | 无 |
| 无 | 55001 | 管理端口 | 无 |
| http://10.100.248.42:8080/jointframe/console/ | 8080 | 管理后台发布 | 无 |
| 10.100.248.43 | 无 | 无 | 80 | 数据交换 | 无 |
| 无 | 55001 | 管理端口 | 无 |
| 10.100.248.44 | 无 | 无 | 1433 | 数据交换 | 无 |
| 无 | 55001 | 管理端口 | 无 |
| 3 | 华南督察局网站 |  | 59.252.101.219 | http://hndc.mep.gov.cn/ | 80 | 系统发布 | http://hndc.mep.gov |

附件2

演习工作任务落实情况表

| **序号** | **任务名称** | **完成时间** | **落实情况** |
| --- | --- | --- | --- |
| **（一）** | **系统核查清理** |
| 1 | 系统清查下线 | 5月20日 | 1. 暂时下线国控重点污染源在线监控系统、办公自动化系统平台。
2. 暂时关闭10.100.248.42、10.100.248.43、10.100.248.44、10.100.248.244、10.100.248.245服务器
 |
| 2 | 互联网发布系统清理 | 5月24日 | 没有需要清理的系统 |
| 3 | 互联网发布系统备案 | 5月27日 | 没有需要新备案的系统 |
| **（二）** | **安全边界防护** |
| 1 | 加强网络边界防护 | 5月20日 | 1、部署有东软网闸离专网与单位内网，并在网闸上配置有安全规则来限制互访2、更新专网出口防火墙硬件设备 |
| 2 | 信息系统核查 | 5月15日 | 完成 |
| **（三）** | **系统安全加固** |
| 1 | 弱口令专项整改 | 5月24日 | 一、OA系统整改：1.密码复杂性检测2、输入密码超过3次，锁定账号10分钟3、XSS跨站脚本等字符过滤方面的漏洞4、限制同一个帐号在同一个时间内只允许在一个地方登录5、密码使用了 md5加密了同时用的是post方式传递C:\Users\admin\AppData\Local\Temp\WeChat Files\8ea3890c54a9767a00c691f6fb647519_.jpgC:\Users\admin\AppData\Local\Temp\WeChat Files\7e0e3777c2a4416ab6a325175e498321_.jpgC:\Users\admin\AppData\Local\Temp\WeChat Files\318ff8487e288bdd7ce04f7c851e6e52_.jpgC:\Users\admin\AppData\Local\Temp\WeChat Files\b03e59a28dc65d2d3f88bae86a9a52e9_.jpgC:\Users\admin\AppData\Local\Temp\WeChat Files\18059e556292dc5e5dd1da8864d1b78a_.jpg二、档案系统整改： |
| 2 | 堡垒主机配置实施 | 5月24日 |  |
| 3 | 系统漏洞整改修复 | 持续开展 |  |
| **（四）** | **监控应急值守** |
| 1 | 实时安全监控 | 持续开展 |  |
| 2 | 应急值守保障 | 持续开展 | （附上应急值守计划，包括本单位及各系统的值班情况） |
| （**五）** | **提高安全意识** |
| 1 | 提高安全意识 | 5月24日 | <http://opencla.cctv.com/2017/06/13/VIDE3QmP7U22B9NWwYybcco5170613.shtml>组织大家观看网络安全视频讲座，提高网络安全意识 |