充分认清当前网络安全严峻形势
认真做好网络安全等级保护工作

省公安厅网络安全保卫总队 徐晓鹏

主 要 内 容

一、公安机关组织开展网络安全保卫工作情况

二、我国网络安全面临的严峻形势

三、切实做好信息安全等级保护工作

四、当前网络安全工作存在的突出问题

五、进一步加强网络安全保障工作

一、公安机关组织开展网络安全保卫工作情况

（一）开展网络安全执法大检查

为贯彻落中央领导同志关于加强网络安全工作的重要指示精神，切实履行国家法律法规赋予公安机关监督、检查、指导重要信息系统安全保护工作的职能，进一步提高重要信息系统和重点网站的安全防护能力，有效应对当前国内外各种网络安全威胁，维护国家安全、公共安全和基础设施安全，公安机关每年开展一次网络安全执法检查。


国家级重要信息系统和重点网站
安全执法检查工作电视电话会议


党政机关、事业单位和国有企业互联网网站安全
专项整治行动电视电话会议

（二）深入推进网络安全等级保护工作

积极推动重点行业、重要部门开展网络安全等级保护工作，加强与各行业主管部门协调沟通，进一步深化重要信息系统定级备案、等级测评及建设整改工作，提高重要信息系统的安全保障能力。全面摸清县级以上政府网站底数，指导帮助各级政府网站开展定级备案工作，建立政府网站安全事件（故）应急处置机制。

。

近年来，在省委、省政府和公安部正确领导下，在各级各有关单位大力支持配合下，全省公安机关大力加强信息网络安全保卫工作，扎实落实各项安保措施，有力维护了全省信息网络安全。目前，全省共备案二级信息系统8346个，三级以上信息系统959个，政府网站3631个，已测评三级系统581个，我省信息网络保持了基本安全的态势。

（三）加强对国家级重要信息系统的安全保障

- 2014年10月13日，公安部与国家发改委、财政部联合下发了《关于加强国家级重要信息系统安全保障工作有关事项的通知》（公信安[2014]2182号）。

- 公安机关在打击网络攻击、等级保护、通报预警、应急处置方面加强保障。

- 国家发改委、财政部在信息安全专项、政府采购、经费方面给与保障。

（四）全面推进网络安全信息通报机制建设 提高监测和预警处置能力

- 中办、国办下发的《关于加强社会治安防控体系建设的意见》、《关于全面深化公安改革若干重大问题的框架意见》中，要求“**完善国家网络安全监测预警和通报处置工作机制**”。
- 2015年公安部召开部省市三级电视电话会议，部署省市公安机关开展网络安全监测预警通报机制建设，推动建立**覆盖部省市三级、115个重要行业、横纵通畅的立体化全国网络安全监测预警通报处置体系。**

国家层面形成了以国家网络与信息安全信息通报中心为核心，65个部委、50家央企为成员，以院士为组长的政府通报机制专家组、央企通报机制专家组、央企通报机制秘书处、4家信息支撑单位、50家技术支撑单位参加的国家网络安全信息通报机制。

2010年8月，省公安厅网安总队加挂“山东省网络与信息安全信息通报办公室”牌子，建立与省委、省政府、通报机制成员单位信息通报机制。2014年以来，编发《网络与信息安全情况通报》30余期，向省直各单位、中央驻鲁各单位及各市公安机关通报全国及山东省内网络病毒情况、安全漏洞情况、网站挂马情况、被篡改网络情况、重大安全事件及信息安全资讯等情况。

（五）加强对政府网站的安全监管

- 2014年3月和5月，公安部向全国公安机关网络安全保卫部门下发了《关于加强政府网站安全监管工作的指导意见》和《公安机关政府网站安全监管工作规范》
- 各地公安机关按照公安部要求，加快开展政府网站梳理、备案、安全监测、通报预警、案事件处置等工作

- 全面开展重点网站安全技术检测

全国政府网站161503个（可正常访问的，含二级域名）。12.9%的网站存在直接被入侵的漏洞、或已被恶意入侵，21.2%的网站存在高危漏洞。

42%的政府网站存在信息泄露、可被间接利用的漏洞等安全隐患。

网安总队于2013年建成全省重点网站安全监测报警平台，对省、市、县三级2000余个重点网站安全情况进行实时监测，2014年以来，通报各地公安机关、政府部门高危网站840个，通过实时监测和安全情况通报制度的建立健全，我省高危政府网站数量减少了75%。各市公安机关均已建成重点网站安全监测预警平台，7个市成立信息安全通报机构，及时编发网络与信息安全情况通报，向本地各部门下发网站漏洞扫描报告和网络安全预警信息，进一步提高了各单位网站预防和阻止网络攻击、入侵的能力。

（六）对地方党委政府进行考核

- 中央综治办印发《2014年综治工作（平安建设）考核评价实施细则》，将“网络安全保障工作”纳入全国综治考核（2分），明确了各级政府的网络安全保障责任。
- 公安部按照中央综治办要求，下发考核要点，组织对地方党委政府的信息安全等级保护、网络安全通报预警、互联网安全管理、网络违法犯罪情况等开展年度考核。

- 2013年省综治委下发《关于印发<山东省社会管理综合治理委员会关于在平安山东建设中加强“网络平安”工作的意见>的通知》（鲁综治〔2013〕9号），进一步明确了网络安全领导组织保障和工作重点。

（七）开展智慧城市网络安全建设和管理

- 公安部会同中央网信办、发改委、工信部，联合出台了《关于加强智慧城市网络安全建设和管理工作的指导意见》（中网办发文[2015]9号），对智慧城市中的网络安全工作提出明确要求。

（八）开展网络攻击违法活动的专项打击

- 93纪念活动前夕，共破获从事网络攻击篡改、侵入控制计算机信息系统、制作传播木马病毒、黑客工具等行为的案件301起，抓获违法犯罪嫌疑人758名。
- 清理僵尸网络控制端和被控计算机7100余台，清理恶意移动程序3．6万余个，删除网站后门、被插入暗链等3万余条，关闭网站、栏目、通讯群组1587个。

（九）加强法律、政策、标准、工程研究

- 在人大法工委组织下，公安部会同有关部门开展《网络安全法》的研究制定；修改完善《反恐怖主义法》和《刑法》修正案
- 开展网络安全“十三五”规划、“十三五”重大工程研究
- 制定云计算、物联网、大数据、工业控制系统、移动互联等新技术的等级保护基本要求、安全设计技术要求和测评要求等技术标准。

（十）完成国家重大活动的网络安保任务

- 组织技术支持队伍，对网络安全重点保卫单位开展渗透性技术检测、实时安全监测
- 落实安全责任制，层层签订责任书。
- 暂时关闭一些无关紧要的网站、网络系统

二、我国网络安全面临的严峻形势

我国国家安全面临的三大威胁

一是战争威胁

二是恐怖威胁

三是网络安全威胁

（一）美国对我网络安全构成最大威胁

- 成立网军司令部，建设数万人网军，研发了数千种网络战武器。举行网络风暴演习，随时可以对我发动网络战。
- 奥巴马近期经常拿美国的网络战能力威胁、恐吓中国，把中国、俄罗斯、伊朗、朝鲜作为其四个主要对手，中国排首位。
- 使用各种方法，利用各种途径对我国家关键信息基础设施进行控制、攻击和窃密。

“棱镜”窃听活动

棱镜计划（PRISM）是一项由美国国家安全局（NSA）自2007年起开始实施的绝密电子监听计划。该计划的正式名号为“US-984XN”。美国情报机构一直在包括微软、雅虎、谷歌、苹果、思科等在内的九家美国互联网公司中进行数据挖掘工作，从音频、视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动。监控的类型有10类：信息电邮，即时消息，视频，照片，存储数据，语音聊天，文件传输，视频会议，登录时间，社交网络资料的细节，其中包括两个秘密监视项目，一是监视、监听民众电话的通话记录，二是监视民众的网络活动。

美国国安局2009年起就开始入侵华为公司深圳总部的服务器，获取公司高层之间的内部通信信息，甚至窃取了华为各产品的保密源代码。国安局的原始目的是，寻找华为与中国军方的关系，但随着时间的推移，开始研究如何入侵华为出售给第三国的计算机和电话网络，想搞清楚如何破解华为的产品。

美国的技术优势

- 美国作为网络发源地，成为全球应用最多、普及最广的因特网的起源地。
- WINDOWS操作系统和INTEL处理器的技术一直掌控在美国手中。
- 美国拥有庞大的网络系统，仅仅国防部网络系统就有700万台电脑，运营有1.5万个计算机网络。其中，与美国陆军、海军、空军、巡航导弹和后勤等有关的网络就高达170多个。美国的网络技术可以说是全球最成熟的。
-

- 全球13个域名根服务器中，唯一的主根服务器在美国，另外12台中有9个在美国，1个在英国，1个在瑞典，1个在日本。美国还控制着网络连接需要的卫星和海底电缆。网络信息流的节点基本上都由美国控制。
- 美国政府在网络安全上的支出每年高达约100亿美元。这是世界上任何一个国家都无法相比的。

（二）敌对势力和黑客组织的严重威胁

- 近年来藏独、疆独、法轮功等敌对势力、敌对组织在美等国的支持下，利用互联网对我政府网站、基础网络、重要信息系统和国家网络关防等进行入侵攻击、控制和突破。
- “反共黑客联盟”、“匿名者”、“电子圣战基地”等黑客组织日益猖狂，攻击篡改我政府网站。

（三）互联网快速发展带来的严重挑战

- 网上大V呼风唤雨，造谣生事，互联网企业、网民、网上舆论左右着社会发展和走向，严重冲击着广播电视、报刊杂志等传统媒体。
- 互联网已成为暴恐活动的重要勾联、指挥平台。
- 网上的QQ、微信、微博等网络应用将新闻媒体从树状结构变成了网状结构，造成网上舆论、信息和行为管理异常困难，极易产生“温水煮青蛙”效果。这是美国策动“颜色革命”的主要手法。

（四）关键信息基础设施安全隐患严重，日益影响国家安全

- 美国“八大金刚”（思科、IBM、谷歌、高通、Inter、苹果、甲骨文、微软）的产品，已深度渗透至我国电信、金融、能源等关键信息基础设施。
- 我重要行业部门选用国外操作系统、数据库、服务器、核心路由器等关键信息产品，这些国外产品很多都被情报机构预置了后门或植入了木马，这些产品中的后门、漏洞客观上成为了窃密渠道和网络攻击的通道。

（五）不法分子利用“互联网+”使网络犯罪升级

- 网络窃密、网络赌博、网络诈骗、网上盗窃等违法犯罪活动日益猖獗。
- 不法分子利用各种手段窃取、贩卖公民个人信息，从事各种违法犯罪活动，被窃取贩卖或泄漏的信息涉及金融、电信、公安、交通、教育、医疗、国土、工商、房产、物业、保险、快递等重要部门和行业。

（六）新技术新应用带来重大风险隐患

- 基于IPv6下一代互联网、物联网、云计算、大数据、移动互联网等新技术正在加快应用到电力、石油、交通等重要行业，逐步实现“智能电网”、“智能油田”和“智慧城市”，推动着我国技术进步和经济发展。
- 云计算、大数据等新技术新应用的自身安全问题日益突显。随着国家信息化建设的加快，关系国计民生的大规模网络、系统以及大数据的安全风险显著增加，更易成为网络攻击的目标，网络安全问题将更加凸显。

- 在大数据时代，数据就是资本、金钱，有数据就有资源；大数据都是关联的，数据到了一定的规模，就不是个人隐私的问题了，而是公共安全问题，就是国家政治安全、经济安全问题。

三、切实做好信息安全等级保护工作

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

信息安全等级保护的三大核心内容

1、对信息系统分等级实行安全保护、按标准进行建设、管理和监督；

2、对信息系统中使用的信息安全产品实行按等级管理；

3、对信息系统中发生的信息安全事件分等级响应、处置。

颁布时间	文件名称	文号	颁布机构	内容及意义
1994年 2月18日	《中华人民共和国计算机信息系统安全保护条例》	国务院147号令	国务院	第一次提出信息系统要实行等级保护，并确定了等级保护的职责单位。
2003年 9月7日	《国家信息化领导小组关于加强信息安全保障工作的意见》	中办国办发[2003]27号	中共中央办公厅 国务院办公厅	等级保护工作的开展必须分步骤、分阶段、有计划的实施。明确了信息安全等级保护制度的基本内容。
2004年 9月15日	《关于信息安全等级保护工作的实施意见》	公通字[2004]66号	公安部 国家保密局 国家密码管理委员会办公室（国家密码管理局） 国务院信息化工作办公室	将等级保护从计算机信息系统安全保护的一项制度提升到国家信息安全保障的一项基本制度。
2007年 6月22日	《信息安全等级保护管理办法》	公通字[2007]43号		明确了信息安全等级保护制度的基本内容、流程及工作要求，明确了信息系统运营使用单位和主管部门、监管部门在信息安全等级保护工作中的职责、任务。
2007年 7月16日	《关于开展全国重要信息系统安全等级保护定级工作的通知》	公信安[2007]861号		就定级范围、定级工作主要内容、定级工作要求等事项进行了通知。

国家对网络安全等级保护制度的新要求

- 2015年中办、国办下发《关于加强社会治安防控体系建设的意见》、《关于全面深化公安改革若干重大问题的框架意见》，要求“**加强信息网络防控网建设。健全信息安全等级保护制度**”。
- 《网络安全法》中明确要求：国家实施网络安全等级保护制度。

《网络安全法》

第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

《网络安全法》

第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

《信息安全等级保护管理办法》第六条、第七条规定，信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。信息系统的安全保护等级分为五级。

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法权益	损害	自主保护
第二级		合法权益	严重损害	指导
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督检查
		国家安全	损害	
第四级		社会秩序和公共利益	特别严重损害	强制监督检查
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专门监督检查

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第一级安全保护能力：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

第二级安全保护能力：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

第五级安全保护能力：（略）。

等级保护工作的主要流程

一是自主定级与审批。信息系统运营使用单位按照等级保护管理办法和定级指南，自主确定信息系统的安全保护等级。有上级主管部门的，应当经上级主管部门审批。跨省或全国统一联网运行的信息系统可以由其主管部门统一确定安全保护等级。在信息系统确定安全保护等级过程中，可以组织专家进行评审。对拟确定为第三级以上信息系统的，运营使用单位或主管部门应当邀请省等保办推荐的等保专家进行评审。第四级以上信息系统的，运营使用单位或主管部门应当邀请国家信息安全保护等级专家评审委员会评审。

二是备案。第二级以上信息系统定级单位到所在地设区的市级以上公安机关办理备案手续。

三是系统安全建设、整改。信息系统安全保护等级确定后，运营使用单位按照管理规范和技术标准进行建设、整改，选择管理办法要求的信息安全产品，建设符合等级要求的信息安全设施，建立安全组织，制定并落实安全管理制度。

四是等级测评。信息系统建设、整改完成后，运营使用单位选择符合管理办法要求的检测机构，对信息系统安全等级状况开展等级测评。

五是监督检查。公安机关依据信息安全等级保护管理规范，监督检查运营使用单位开展等级保护工作，定期对第三级以上的信息系统进行安全检查。运营使用单位应当接受公安机关的安全监督、检查、指导，如实向公安机关提供有关材料。

- 开展信息安全等级保护测评体系建设。部、省两级公安机关认真组织开展等级测评机构能力验证、测评师培训考核。

全国共审核推荐了141家信息安全等级测评机构，覆盖全国31个省、自治区、直辖市（除西藏以外）。

全国获得等级测评师证书的人数达到3674人，其中初级测评师2449人，中级测评师891人，高级测评师334人。

2015年1月，由公安部信息安全等级保护评估中心、电力行业信息安全等级保护测评中心、国家信息技术安全研究中心等9家测评机构联合发起成立了“中关村信息安全测评联盟”，并开展卓有成效的工作。

- 规范测评活动，提高测评技术能力和服务质量，支持配合公安网安部门推进信息安全等级保护工作，为各行业部门提供咨询、技术支持等服务。

- 引导支持技术创新，积极开展新技术和新应用下的测评方法研究、工具研发、成果转化和市场推广，促进联盟的技术升级和产业持续发展。
- 依托中关村科技创新基地，发挥政策优势和集群效应，加强与政产学研各界的合作与交流，努力促进联盟成长为我国最具权威的信息安全技术的核心力量。

- 2015年9月组织开展了能力验证工作。全国119家测评机构（不包括推荐未满一年的测评机构）参加了能力验证活动，参与人员总数达400余人。

  经验证，有105家测评机构通过，通过率达到88.24%。


2015年公安部组织全国测评机构进行能力验证考核
“CNAS T0805 信息系统安全等级保护测评”能力验证活动

山东省测评公司名单

1	山东新潮信息技术有限公司
2	联通系统集成有限公司
3	山东维平信息安全测评技术有限公司
4	青岛速科评测实验室有限公司
5	山东省计算中心
6	山东省电子信息产品检验院
7	济南时代确信信息安全有限公司
8	山东电信集成有限责任公司
9	浪潮软件集团有限公司
10	济南三泽信息安全测评有限公司

四、当前网络安全工作存在的突出问题

一是认识不到位，工作合力尚未形成

一些单位部门和地方政府领导对网络空间的迅速发展变化、影响国家政治安全的程度，面临的严峻形势、严重威胁，自身存在的突出问题等看不清，认识不到位。

二是基础设施建设严重依赖国外

我们信息化建设是先发展后管理，先发展后安全，加上我们采取大量引进、跨越式发展模式，决定我们需要大量引进西方的核心技术和一些基础设施。2012年我国进口的电子芯片是2600多亿，超过我们的石油进口，石油进口是2300多亿，这说明我们在基础设施上对国外严重依赖。

三是关键信息基础设施安全防护能力较弱

保障国家关键信息基础设施安全是敌我网上斗争的重要内容，更是常态化的、动态化攻防能力的较量。我国实施的金盾、金关、金财、金税、金审、金农等12金工程，以及全民社会保障、安全生产监管、金融监管、能源安全保障等15个大型信息化建设工程，建设了电子政务外网、公安专网、税务专网等近百个大型业务专网，以及卫星定位系统、国家自然资源和地理空间基础信息库、人口管理系统等近10万个生产、控制、指挥、调度等大型业务信息系统，这些国家关键信息基础设施面临的网络攻击破坏与窃密、甚至网络恐怖袭击的风险威胁也在不断加大。然而，我国关键信息基础设施在法律、资金、人员、技术、产品等安全保障不足，网络安全防护能力差，应对网络威胁的能力整体不足，无法抵御大规模、有组织的网络攻击。

四是监管力度不强

国家层面对网络安全工作落实情况监管力度不强，对发生的重大网络安全案事件（事故）问责追责不够，已有法律、政策、战略、标准、规范缺乏有效落实。一方面一些重点行业部门、大型服务网站和互联网服务商没有按照国家有关要求落实安全管理措施和技术保护措施，导致国家大量机密、商业秘密、公民信息频遭窃取；另一方面，部分互联网产品和服务提供商没有落实应尽的责任和义务，有的为网络犯罪活动客观上提供了便利。

五是资金投入不足

政府部门关键信息基础设施安全保护没有专门经费，企业在网络安全方面投入的资金不足，关键信息基础设施安全保护工作的连续性得不到保障，部分网络设备得不到升级更新。

五、进一步加强网络安全保障工作

（一）提高网络安全保护认识

2014年2月27日，中央网络安全和信息化领导小组成立，习总书记亲自担任组长。领导小组着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

习近平总书记指出：

- “没有网络安全，就没有国家安全；没有信息化，就没有现代化”
- “网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施”
- 网络强国战略目标：“技术要强、内容要强、基础要强、人才要强、国际话语权要强”
- 网络安全关系到：意识形态、技术、数据、应用、边防、资本、渠道安全

第二届世界互联网大会习近平主席提出五点主张：

- 加快全球网络基础设施建设，促进互联互通
- 打造网上文化交流共享平台，促进交流互鉴
- 推进网络经济创新发展，促进共同繁荣
- 保障网络安全，促进有序发展
- 构建互联网治理体系，促进公平正义

- 目前网上斗争的总体形势是敌强我弱，表现为“四个没有根本转变”：

一是美国垄断网络霸权的格局没有根本改变

二是网络空间敌强我弱的总体态势没有根本转变

三是敌对势力妄图利用网络“扳倒中国”的政治图谋没有根本改变

四是我技术上受制于人的被动局面没有根本改变。

（二）积极开展信息安全等级保护工作

信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，为提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展而实施的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，增强信息安全保护的整体性、针对性和实效性，促进我省信息安全的发展。

（三）加强网络与信息安全信息通报工作

落实党中央“完善国家网络安全监测预警和通报处置工作机制”要求以及2015年1月6日下发的《关于加快推进网络与信息安全信息通报机制建设的通知》（公信安[2015]21号）要求。开展两项基本建设：

- 建立省、市两级网络安全信息通报中心

我省目前已建立的通报机构，省级：省网络与信息安全信息通报办公室；市级：济南、淄博、潍坊、济宁、临沂、滨州、泰安均已建立市网络与信息安全信息通报办公室

- 建立完善网络安全通报预警机制

将军队、安全等信息情报部门，发改、教育、科技、财政、商务、人社、国土、保密、密码等政府职能部门，工商、税务、银行、电力、证监、保监、质检、交通、水利、文化、卫生、体育、农业等重要行业主管部门、以及重要国企纳入信息通报机制成员单位。建立通报机制专家组，建立通报机制技术支持单位，构建以公安网安部门为中心，通报机制成员单位、专家组和技术支持单位参加的本地信息通报机制。

谢谢!